Source: Business Law/Internet Law and Practice in California/Contents

Contents

Volume 1

Preface

About the Authors

About the Contributing Authors

About the 2010 Update Authors

Selected Developments

Cutoff Dates and CEB Citation

Intellectual Property Rights in Cyberspace

1 Copyrights and the DMCA

2 Patents and Trade Secrets

3 Domain Names and Trademark Issues

Human Resources

4 Human Resources

Launching and Operating a Website

5 Website Development

6 Hosting and Related Services

7 Electronic Contracting

8 Terms of Use; Online Agreements; Linking; Downloading

9 Privacy Law and Privacy Policies

10 E-Commerce Transactions and Tax Issues

11 Strategic Alliances

12 Software License Agreements

Volume 2

Licensing and Other Collaborative Arrangements

13 Software Development Agreements

14 Content Clearances, Licensing, and Fair Use

15 Source Code Escrows

Financing an Online Business

16 Financing an Online Business

Advertising on the Internet

17 Advertising on the Internet

Liability and Litigation Issues

18 Viruses and Other Network Disruptions

19 Jurisdiction; Conflicts of Law

20 Tort and Criminal Liability; First Amendment Issues; Insurance

20A Discovery of Electronically Stored Information

International Issues

21 International Issues

Acquisitions and Sales of Internet-Based Businesses

22 Acquisitions and Sales of Internet-Based Businesses

Internet Resources for California Businesses

Table of Statutes, Regulations, and Rules

Table of Cases

Table of References

Table of Forms

Index

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/Preface

Preface

The Internet has transformed the global economy. Internet Law and Practice in California represents CEB's response to the explosive growth of the Internet over the last 15 years and the attendant development of an entirely new field of law concerning business and personal interactions online. This book is intended to be a practical reference manual for counsel representing California businesses or individuals who now operate or wish to develop commercial Internet websites or who otherwise transact business online. The book includes dozens of useful forms, and throughout the text are many valuable Practice Tips. The authors discuss major federal and state statutory and regulatory developments concerning the Internet and relevant cases decided by federal and state courts in California. In addition, the book includes a directory of Internet resources for California businesses. This book is not intended to replace the nationally oriented multivolume intellectual property treatises, but rather to serve as a useful handbook for practicing California attorneys.

The chapters of this book fall into nine major subdivisions:

- Chapters 1, 2, and 3 provide an overview of intellectual property rights in cyberspace, including copyrights, the Digital Millennium Copyright Act, patents, trade secrets, domain names, trademarks, metatags, and trade dress.
- Chapter 4 covers human resource issues relating to online businesses, including employees, independent contractors, and advisory boards.
- Chapters 5 through 10 address legal issues arising in connection with launching and operating a website. The topics include acquisition of intellectual property, website development, web hosting and co-location agreements, service level agreements, technical support, electronic contracting, terms of use, online software license agreements, linking arrangements, downloading and uploading content, privacy law, website privacy policies, e-commerce transactions, and Internet taxation.
- Chapters 11 through 15 address licensing and other collaborative arrangements, including strategic alliances, software license agreements, software development agreements, content clearing, content licensing and fair use, and source code escrows.
- Chapter 16 presents an overview of financing issues for online businesses, including start-up equity financing, debt financing, and security interests in intellectual property.
- Chapter 17 covers advertising on the Internet, including federal and state advertising regulation, Federal Trade Commission guidelines, unsolicited commercial email (spam), and Internet advertising agreements.
- Chapters 18 through 20A address liability and litigation issues, including viruses and other network disruptions, Internet jurisdiction, tort and criminal liability, First Amendment issues, Internet complaint sites, insurance, and discovery of electronically stored information.
- Chapter 21 provides an overview of selected international issues, including jurisdictional issues, content regulation, European Union Directives, and U.S. export controls.
- Chapter 22 reviews selected legal issues regarding acquisitions and sales of Internet-based businesses, including intellectual property due diligence, representations and warranties covering intellectual property, and procedures for changing ownership of domain names.

For a detailed summary of the contents of each chapter, see the chapter outline at the beginning of each chapter. The chapter outlines list each section heading and provide a sequential preview of the topics covered in each chapter.

CEB gratefully acknowledges the work of the lead authors of this book, Clara Ruyan Martin and David B. Oshinsky, and their contributing authors, Dawn C. Anaiscourt, Lilian K. Hanna, Sanjay Jose Mullick, Michael L. Pigott, and Matthew L. Steimel. CEB also gratefully acknowledges the work of the authors of Chapter 20A, Alexander H. Lubarsky and Russell H. Jackman. Each of the authors gave generously of his or her knowledge and specialized skills. See About the Authors and About the Contributing Authors on the following pages for biographical information. Finally, CEB thanks Marla A. Hoehn and Carrie M. LeRoy, of Pillsbury Winthrop LLP, Palo Alto for their contributions; some material from their article *Website User Agreements: Electronic Contracting Issues and Tips for Drafting*, 18 CEB Cal Bus L Prac 10 (Winter 2003), was used in the preparation of Chapter 7 of this book.

CEB attorney Suzanne L. Weakley was in charge of this project. Legal editing was performed by Sally St. Lawrence, Ann Davis,

and Jean Magistrale. Further legal research assistance was provided by Sally St. Lawrence.

The book was designed by Grier Thornburg. Richard Dempewolf copyedited this book and supervised production. The index was prepared by Robert W. Burke, Jenny Jones, and Kathryn Te Selle. Composition was performed by CEB's Electronic Publishing staff.

May 2010 Update

Professor Jack Lerner, of the University of Southern California, Gould School of Law, was the Executive Editor of this update. The authors of this update were Clara Ruyan Martin, Professor Lerner, Alexander H. Lubarsky, Sanjay Jose Mullick, and Ada L. Loo. Professor Lerner and Ms. Martin wish to acknowledge and thank USC law student Brianna Dahlberg for her assistance in research and writing for this update.

CEB Attorney Editor Suzanne L. Weakley and Legal Editor Sally St. Lawrence contributed to this update. Administrative support was provided by Kenya Denman and Nila Kanzaria. Linda Marousek handled copyediting and production. The index was updated by Kathryn Te Selle. Composition was performed by CEB's Electronic Publishing staff.

Michael Fenger
Practice Group Manager
Business Law

Pamela J. Jester
Director

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/About the Authors

About the Authors

CLARA RUYAN MARTIN received her B.A. degree from the University of California (Berkeley) in 1985 and her J.D. degree from the University of Michigan Law School in 1989. She is a founding partner of the Los Angeles law firm, Cadence Law Group LLP. She specializes in structuring, drafting, negotiation and implementation of corporate and technology transactions. Her corporate work includes mergers and acquisitions, joint ventures, corporate finance, and venture representation. Her technology practice is broad, ranging from software licensing and development to strategic alliances and e-commerce. Ms. Martin has served on the Cyberlaw Committee of the State Bar of California and is a frequent lecturer on topics such as software licensing agreements, Internet-related agreements, complex joint ventures, venture finance, and mergers and acquisitions.

DAVID B. OSHINSKY received his B.A. degree from Yale University in 1991 and his J.D. degree from Columbia Law School in 1996, where he was a member of the *Columbia Law Review*. He is a founding partner of the Los Angeles law firm, Cadence Law Group LLP. Mr. Oshinsky works with many start-up and early stage companies, for which he provides counsel regarding their early operational, financing, and intellectual property requirements. He regularly assists clients with venture capital financing, technology transactions, and mergers, acquisitions and related corporate transactions. In particular, his practice involves the structuring, drafting, and negotiating of technology licenses, website policies and agreements, software development agreements, and strategic alliances. Mr. Oshinsky has written and lectured on a broad range of technology topics, including website development agreements, strategic alliances, intellectual property issues in mergers and acquisitions, and Internet law in California.

© The Regents of the University of California

About the 2010 Update Authors

JACK LERNER received his B.A. with distinction from the University of Kansas and his J.D. from Harvard Law School, where he was an editor of the Harvard Environmental Law Review. He clerked for the Honorable Fred I. Parker of the U.S. Court of Appeals for the Second Circuit and for the Honorable G. Thomas Van Bebber of the U.S. District Court for the District of Kansas. Professor Lerner is Visiting Clinical Assistant Professor of Law at the University of Southern California, Gould School of Law, and from 2007 to 2008 was Acting Director of the USC Intellectual Property and Technology Law Clinic. Previously, he was a clinical fellow at the Samuelson Law, Technology & Public Policy Clinic of the University of California, Berkeley, School of Law, and before that practiced intellectual property litigation with Wilson Sonsini Goodrich & Rosati, P.C. in Palo Alto. In 2004, he was a research fellow with the Berkman Center for Internet & Society at Harvard Law School. Professor Lerner is the Executive Editor of this update and the 2010 update author of Chapters 1 and 14.

ADA L. LOO received her B.A. in political science from Emory University in 1994 and her J.D. from American University's Washington College of Law in 2001. She is an international trade associate at Pillsbury Winthrop Shaw Pittman LLP in Washington, D.C., where her practice focuses on U.S. export controls that involve the regular application of the Export Administration Regulations, the International Traffic in Arms Regulations, and the Office of Foreign Assets Control Regulations before the U.S. Departments of State, Commerce, Treasury, and Defense. She advises clients on internal corporate compliance programs, license approvals, and encryption software and technology reviews, as well as a number of customs law matters such as rules of origin, tariff classification, valuation, and duty drawback issues. Ms. Loo is the 2010 update co-author of §§21.21-21.61 (on U.S. export controls) of Chapter 21.

ALEXANDER H. LUBARSKY received his B.A. degree from Lewis and Clark College and his J.D. and L.L.M. degrees from Golden Gate University School of Law. Mr. Lubarsky is a practicing litigator, electronic discovery consultant, and author. He has litigated hundreds of cases involving electronic discovery and has received numerous awards in the industry, including the TechnoLawyer @ Award. Mr. Lubarsky has been elected to the Executive Committee of the Law Practice Management and Technology Section of the State Bar of California and is on the editorial boards of several technology publications. He has consulted for numerous companies that provide electronic discovery support services, including Summation Legal Technologies, Inc.; Fios, Inc.; Guidance Software, Inc.; Daticon, LLC; and Zantaz, Inc. Mr. Lubarsky regularly consults with large law firms and Fortune 500 corporations in the area of ESI retention, e-discovery best practices, and litigation holds. Mr. Lubarsky is the 2010 update author of Chapter 20A.

CLARA RUYAN MARTIN received her B.A. degree from the University of California (Berkeley) in 1985 and her J.D. degree from the University of Michigan Law School in 1989. She is a founding partner of the Los Angeles law firm Cadence Law Group LLP. She specializes in structuring, drafting, negotiation, and implementation of corporate and technology transactions. Her corporate work includes mergers and acquisitions, joint ventures, corporate finance, and venture representation. Her technology practice is broad, ranging from software licensing and development to strategic alliances and e-commerce. Ms. Martin has served on the Cyberlaw Committee of the State Bar of California and is a frequent lecturer on topics such as software licensing agreements, Internet-related agreements, complex joint ventures, venture finance, and mergers and acquisitions. Ms. Martin is the 2010 update author of Chapters 2-13, Chapters 15-20, §§21.1-21.20 of Chapter 21, and Chapter 22.

SANJAY JOSE MULLICK received a B.S.F.S degree from Georgetown University School of Foreign Service in 1991 and a J.D. degree from Georgetown University Law Center in 1996. He is counsel in the International Trade group at Pillsbury Winthrop Shaw Pittman LLP and practices in its Washington, D.C., office. He specializes in international dispute resolution and international trade regulation, advising both companies and governments. He also counsels companies on compliance with U.S. export controls, with an emphasis on technology-related issues such as encryption and outsourcing. He is a member of the District of Columbia Bar International Trade Planning Committee. Mr. Mullick is the 2010 update co-author of §§21.21-21.61 (on U.S. export controls) of Chapter 21.

© The Regents of the University of California

About the Contributing Authors

DAWN C. ANAISCOURT received a J.D. from the University of California, Los Angeles, School of Law in 2000, an M.B.A. from the University of California (Los Angeles) in 2000, and a B.A. from Harvard University in 1988. She is an associate at the Los Angeles office of the law firm of Katten Muchin Zavis Rosenman. She practices in the areas of corporate and securities and mergers and acquisitions. Her clients includes start-ups, pre-IPO companies, and public corporations. Ms. Anaiscourt is a contributing author for Chapters 1 (Copyrights and the DMCA), 4 (Human Resources), 8 (Terms of Use, Online Agreements, Linking, Downloading), 10 (E-Commerce Transactions and Tax Issues), 19 (Internet Jurisdiction), and 20 (Liability Issues).

LILIAN K. HANNA received her J.D. degree in 2001 from the University of Southern California School of Law and her undergraduate degree in 1998 from the University of California (Irvine). She practices in Los Angeles in the areas of corporate and intellectual property law, advising clients on a wide range of business and technology transactions. Ms. Hanna is a contributing author for Chapters 2 (Patents and Trade Secrets), 3 (Domain Names and Trademark Issues), 4 (Human Resources), 8 (Terms of Use, Online Agreements, Linking, Downloading), 13 (Software Development Agreements), 14 (Content Clearances, Licensing, and Fair Use), 15 (Source Code Escrows), and 20 (Liability Issues).

RUSSELL H. JACKMAN completed his undergraduate work at the University of California (San Diego) in 1985 and received his J.D. degree from the McGeorge School of Law in Sacramento in 1990. He is owner of Community Legal Automation Software and Services (CLASS). CLASS provides legal technology consulting services to law offices throughout California, including software sales, seminars, lectures, and private consultations regarding upgrading and maximizing law office technology usage and PowerPoint trial presentations. Mr. Jackman has been a member of the Law Practice Management and Technology Section of the State Bar of California since 1996 and served as vice-chair of the committee in 2004. He is a frequent speaker on the topics of computer technology in the law office, computer security, and trial presentations at programs sponsored by the State Bar of California and other organizations. Mr. Jackman is the co-author of Chapter 20A (Discovery of Electronically Stored Information).

ALEXANDER H. LUBARSKY received his B.A. degree from Lewis and Clark College and his J.D. and L.L.M. degrees from Golden Gate University School of Law. Mr. Lubarsky is a practicing litigator, electronic discovery consultant, and author. He has litigated hundreds of cases involving electronic discovery and has received numerous awards in the industry, including the TechnoLawyer @ Award. Mr. Lubarsky has been elected to the Executive Committee of the Law Practice Management and Technology Section of the State Bar of California and is on the editorial boards of several technology publications. He has consulted for numerous companies that provide electronic discovery support services, including Summation Legal Technologies, Inc.; Fios, Inc.; Guidance Software, Inc.; Daticon, LLC; and Zantaz, Inc. Mr. Lubarsky regularly consults with large law firms and Fortune 500 corporations in the area of ESI retention, e-discovery best practices, and litigation holds. Mr. Lubarsky is the co-author of Chapter 20A (Discovery of Electronically Stored Information).

SANJAY JOSE MULLICK received a B.S.F.S degree from the Georgetown University School of Foreign Service in 1991 and a J.D. degree from the Georgetown University Law Center in 1996. He is counsel in the International Trade group at Pillsbury Winthrop Shaw Pittman LLP and practices in its Washington, D.C., office. He specializes in international dispute resolution and international trade regulation, advising both companies and governments. He also counsels companies on compliance with U.S. export controls, with an emphasis on technology-related issues such as encryption and outsourcing. He is a member of the District of Columbia Bar International Trade Planning Committee. Mr. Mullick is the author of §§21.21-21.61 in Chapter 21 on United States export controls.

MICHAEL L. PIGOTT earned a B.A. from Tulane University in 1997 and a J.D. from the University of Southern California Law School in 2001. His practice is focused in the areas of corporate securities, mergers and acquisitions, and intellectual property law. He is currently part of the corporate team at the law firm of Newmeyer & Dillion LLP, Santa Monica. Mr. Pigott is a contributing author for Chapters 1 (Copyrights and the DMCA), 2 (Patents and Trade Secrets), 4 (Human Resources), and 21 (International Issues).

MATTHEW L. STEIMEL received a B.S. in finance from Miami University of Ohio in 1979 and a J.D., cum laude, from The Ohio State University College of Law in 1982. He is Senior Counsel at K&R Law Group LLP in Los Angeles. Mr. Steimel specializes in corporate and healthcare law with an emphasis on mergers and acquisitions, venture capital and other private equity finance, and securities law. In addition, he regularly advises clients on LLC and corporate structuring, formation, and governance and managed care and physician contracting. Mr. Steimel has extensive experience working with both public and private companies, and private equity investors and their portfolio companies, in transactions across a range of industries. Mr. Steimel is a contributing author for Chapters 4 (Human Resources) and 16 (Financing an Online Business).

© The Regents of the University of California

Selected Developments

May 2010 Update

In *Moberg v 33T LLC* (D Del 2009) 666 F Supp 2d 415, the federal district court held that a work posted on a foreign website was not "published" in the United States for purposes of 17 USC §411. See §1.8A.

In *Cincom Sys., Inc. v Novelis Corp.* (6th Cir 2009) 581 F3d 431, the Sixth Circuit found that corporate merger and acquisition transactions may result in violations of non-transferable copyright licenses. See §§1.9, 22.2.

In *Vernor v Autodesk, Inc.* (WD Wash 2009) 93 USPQ2d 1336, the federal district court rejected recent Ninth Circuit decisions on the difference between an owner and a licensee, instead relying on conflicting precedent set by *U.S. v Wise* (9th Cir 1977) 550 F2d 1180. See §1.16B.

The Ninth Circuit held that a defendant domain registrant was not entitled to the safe harbor defense under the Anticybersquatting Consumer Protection Act (ACPA) because it was unlikely that the registrant legitimately believed that his use of the domain name at issue was "wholly lawful." *Lahoti v VeriCheck, Inc.* (9th Cir 2009) 586 F3d 1190, 1203. See §3.23.

In *Louis Vuitton Malletier, S.A. v Akanoc Solutions, Inc.* (ND Cal 2008) 591 F Supp 2d 1098, a federal jury in California awarded $32 million in damages for contributory trademark infringement. See §3.60.

The Second Circuit found that using a competitor's trademarks as a trigger for search-related advertising is a "use in commerce" within the meaning of the Lanham Act and is, therefore, actionable. *Rescuecom Corp. v Google, Inc.* (2d Cir 2009) 562 F3d 123. See §3.73.

In ruling on the validity of a browse-wrap agreement, courts consider primarily "whether a website user has actual or constructive knowledge of a site's terms and conditions prior to using the site." *Hines v Overstock.com, Inc.* (ED NY, Sept. 8, 2009, No. 09 CV 991) 2009 US Dist Lexis 81204. See §7.4.

In *PDC Labs., Inc. v Hach Co.* (CD Ill, Aug. 25, 2009, No. 09-1110) 2009 US Dist Lexis 75378, the court held that a limitation of damages clause in a commercial agreement was not procedurally unconscionable and was therefore enforceable, despite the fact that it was only readable by clicking through a hyperlink embedded in the terms and conditions. See §7.4.

In May 2009, the American Law Institute approved the Proposed Final Draft of its Principles of the Law of Software Contracts (Principles), the purpose of which is to "guide courts in deciding disputes involving transactions in software and to guide those drafting software contracts." See §7.12.

In *In re Sears Holdings Mgmt. Corp.* (June 4, 2009) FTC File No. 082 3099, the FTC brought charges against Sears Holdings Management Corporation (SHMC) for failing to disclose that it used tracking software in connection with its sears.com and kmart.com websites to monitor users' Internet activities. See §9.6.

The Guides Concerning the Use of Endorsements and Testimonials in Advertising (16 CFR §§255.0-255.5) has been revised to include bloggers as marketers required to disclose material connections to advertisers and define endorsements as synonymous with testimonials. See §17.7A.

The misdemeanor provisions of the Computer Fraud and Abuse Act (CFAA) have been held unconstitutionally vague where the alleged violation is based on the defendant's intentional violation of a website's terms of service. *U.S. v Drew* (CD Cal 2009) 259 FRD 449. See §18.5.

An employee who, after receiving notice of termination, used his computer to e-mail documents to himself from his company account was not liable for unauthorized use of a computer under the CFAA. *LVRC Holdings LLC v Brekka* (9th Cir 2009) 581 F3d 1127. See §18.7.

A federal jury in New Jersey determined that a violation of the Electronic Communications Privacy Act (ECPA) occurred when the defendant, through its managers and without authorization, knowingly, intentionally, or purposefully accessed the "Spec-Tator," a group on MySpace.com for past and present employees of Houston's Restaurant, to "vent" about their employer. *Pietrylo v Hillstone Restaurant Group* (D NJ, Sept. 25, 2009, No. 06-5754) 2009 US Dist Lexis 88702. See §18.11.

A federal district court held that Google had no liability to plaintiffs harmed as a result of clicking on allegedly fraudulent web-based advertisements for mobile subscription services. *Goddard v Google, Inc.* (ND Cal 2009) 640 F Supp 2d 1193. See §20.6B.

A distributor of Internet security software was entitled to immunity under 47 USC §230(c)(2) in a suit claiming that its security software interfered with the use of a third party's downloadable programs. *Zango, Inc. v Kaspersky Lab, Inc.* (9th Cir 2009) 568 F3d 1169. See §20.6D.

Attorneys seeking discovery of e-mails have an obligation to craft the appropriate keywords carefully, with input from the ESI's custodians. *William A. Gross Constr. Assocs., Inc. v American Mfrs. Mut. Ins. Co.* (SD NY 2009) 256 FRD 134. See §20A.4.

Failure to promptly notify the party in possession of privileged material may result in a waiver of privilege. See *Brookdale Univ. Hosp. & Med. Ctr., Inc. v Health Ins. Plan of Greater N.Y.* (ED NY, Feb. 13, 2009, No. 07 CV 1471) 2009 US Dist Lexis 11537. See §20A.9.

Effective August 14, 2009, the California Judicial Council amended the Rules of Court to add discovery of electronically stored information to the topics on which parties must meet and confer before their initial case management conference. Cal Rules of Ct 3.724(8). See §20A.17.

California's Electronic Discovery Act (Stats 2009, ch 5), effective June 29, 2009, amended the Civil Discovery Act (CCP §§2016.010-2036.050) to define electronically stored information (see CCP §2016.020(d)-(e)) and make it fully amenable to inspection, duplication, testing, or sampling by any party to a legal action (see CCP §2031.010(a)). See §§20A.18-20A.18E.

A party can be put on notice to preserve data long before litigation is initiated. *Goodman v Praxair Servs., Inc.* (D Md 2009) 632 F Supp 2d 494. See §20A.21.

Loss or destruction of evidence due to "failure to collect evidence, or the sloppiness of the review" may be found grossly negligent or willful. *Pension Comm. of Univ. of Montreal Pension Plan v Banc of Am. Sec.* (SD NY, Jan. 15, 2010, No. 05 CIV 9016) 2010 US Dist Lexis 1839, *10. See §20A.33.

A new breed of "early case assessment" platforms allow a user to look at a particular document and code it by categorizing it as privileged or nonprivileged and indicating what issues the document may help prove or disprove. See §20A.46.

The Article 29 Working Party, a committee of Europe's data protection regulators, issued an opinion advising social networking sites that they must comply with the EU Data Protection Directive if they handle personal data of EU residents. See §21.11.

Six companies agreed to settle FTC charges of unfair and deceptive business practices for representing that they held current certifications to the safe harbor program even though they had allowed their certifications to lapse. See §21.12.

© The Regents of the University of California

Cutoff Dates and CEB Citation

Cutoff Dates

We completed legal editing and analysis of authorities cited in this publication as of February 5, 2010, and monitored developments through March 22, 2010.

CEB Citation

Cite this publication as: Internet Law and Practice in California (Cal CEB 2004).

© The Regents of the University of California

1

Copyrights and the DMCA

I. COPYRIGHTS
- A. Introduction §1.1
- B. Subject Matter of Copyright Law §1.2
- C. Creation and Term of Copyright §1.3
- D. Ownership of Copyrighted Work, Joint Works, and Works Made for Hire
  - 1. Joint Works §1.4
  - 2. Works Made for Hire §1.5
- E. Rights of Copyright Holder §1.6
  - 1. Reproduction Rights §1.6A
  - 2. Distribution Rights §1.6B
  - 3. Performance Rights §1.6C
- F. Copyright Notice §1.7
- G. Copyright Registration
  - 1. Advantages of Registration §1.8
  - 2. Registration Procedures §1.8A
  - 3. When to Register §1.8B
- H. Preregistration §1.8C
- I. Transfer of Copyrights
  - 1. Generally §1.9
  - 2. Form: Copyright Assignment §1.10
  - 3. Form: U.S. Copyright Office Cover Sheet §1.11
- J. Infringement
  - 1. Generally §1.12
  - 2. Direct, Contributory, and Vicarious Liability
    - a. Generally §1.13
    - b. Direct Infringement §1.14
    - c. Contributory Infringement §1.15
    - d. Vicarious Infringement §1.16
    - e. Inducement §1.16A
  - 3. Safe Harbor for Certain Copies of Computer Programs §1.16B
  - 4. Remedies §1.17
- K. Fair Use
  - 1. Introduction §1.18
  - 2. Purpose and Character of Use §1.19
  - 3. Nature of Copyrighted Work §1.20
  - 4. Portion of Work Used §1.21
  - 5. Effect of Use on Market §1.22
- L. First Sale §1.23

II. DIGITAL MILLENNIUM COPYRIGHT ACT
- A. Introduction §1.24
- B. Anti-Circumvention of Technological Protection Measures
  - 1. Anti-Circumvention Prohibitions (17 USC §1201) §1.25
  - 2. Copyright Management Information (17 USC §1202) §1.25A
  - 3. Exceptions to Anti-Circumvention Prohibitions §1.26
  - 4. Remedies §1.27
  - 5. Constitutional Issues: *U.S. v ElCom Ltd.* §1.28
- C. Limitations of Liability for Online Service Providers—Infringement Safe Harbors §1.29
  - 1. General Conditions for Safe Harbors §1.30
  - 2. Transitory Digital Network Communications Safe Harbor (17 USC §512(a)) §1.31
  - 3. System Caching Safe Harbor (17 USC §512(b)) §1.32
  - 4. Safe Harbor for Information Residing on Systems or Networks at Direction of Users (17 USC §512(c))
    - a. Generally §1.33
    - b. Designation of Agent to Receive Notifications §1.34
    - c. "Right and Ability to Control" §1.35
    - d. Removal or Disabling Access to Infringing Material §1.36
    - e. Notification of Claimed Infringement; Safeguards Against Fraudulent Infringement Claims §1.37

f. Counter-Notification by Subscriber; Restoration of Material §1.38
g. Checklist: Notice and Take-Down Checklist §1.39
5. Information Location Tools Safe Harbor (17 USC §512(d)) §1.40
D. Subpoena Power (17 USC §512(h)) §1.41
E. Impact on Internet Service Providers §1.42
F. Checklist: Company DMCA Compliance Policy §1.43

© The Regents of the University of California

I. COPYRIGHTS

§1.1 A. Introduction

Copyright law is the area of intellectual property law most directly implicated by online commerce. The widely reported problems of software and entertainment companies trying to control unauthorized copying and distribution of their copyrighted works (see §§8.21-8.24) illustrate the importance of copyright law to companies doing business on the Internet.

Legislation such as the Digital Millennium Copyright Act (Pub L 105-304, 112 Stat 2860) (see generally §§1.24-1.43) further underscores the central role that copyright law plays in the digital economy. The ease with which copyrighted works can be obtained, reproduced, and distributed online makes a basic understanding of copyright law essential for any business operating online. Because copyrights are protected under federal law even without formal registration, copyright is probably the most often utilized form of intellectual property protection.

The genesis of United States copyright law is US Const art I, §8, which provides that "[t]he Congress shall have power… to promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries." Current federal copyright law is embodied in the Copyright Revision Act of 1976 (the "Copyright Act" or "the Act"), codified at 17 USC §§101-1332. Sections 1.2-1.23 provide an introduction to federal copyright law, registration of copyrights, copyright infringement, and the concept of fair use. For further general discussion of copyright law, including the law applicable to works created before January 1, 1978, see California Business Litigation, chap 7 (Cal CEB 2002). See generally Nimmer, Nimmer on Copyright: A Treatise on the Law of Literary, Musical and Artistic Property, and the Protection of Ideas (1963).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/1 Copyrights and the DMCA/§1.2 B. Subject Matter of Copyright Law

§1.2 B. Subject Matter of Copyright Law

Copyright law protects "original works of authorship" that are fixed in a tangible form of expression from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device. 17 USC §102. It is important to understand that copyright protects only the tangible expression of ideas, not the ideas themselves. As §102 provides:

> In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work.

Therefore, while a computer program written on an electronic storage medium or the graphic images and text that comprise a website may be protectible subject matter under copyright law, the ideas, concepts, and methods embodied in them are not. See, *e.g., Lotus Dev. Corp. v Borland Int'l, Inc.* (1st Cir 1995) 49 F3d 807, aff'd (1996) 516 US 233 (set of menu commands and menu structure was uncopyrightable "method of operation" within 17 USC §102(b), although screen displays and underlying computer code might be copyrightable); *Ashton-Tate Corp. v Ross* (9th Cir 1990) 916 F2d 516 (list of computer commands not copyrightable). As the Ninth Circuit has stated (*Johnson Controls, Inc. v Phoenix Control Sys., Inc.* (9th Cir 1989) 886 F2d 1173, 1175 (citations omitted)):

> Computer software is subject to copyright protection. A computer program is made up of several different components, including the source and object code, the structure, sequence and/or organization of the program, the user interface, and the function, or purpose, of the program. Whether a particular component of a program is protected by a copyright depends on whether it qualifies as an "expression" of an idea, rather than the idea itself.

See also *Iconix, Inc. v Tokuda* (ND Cal 2006) 457 F Supp 2d 969, 996. Ideas and methods, however, may be protectible under trade secret or patent law, as discussed in §§2.3, 2.21-2.22.

It is also important to note that copyright law does not protect facts or raw data. *Feist Publications, Inc. v Rural Tel. Serv. Co*. (1991) 499 US 340, 113 L Ed 2d 358, 111 S Ct 1282; *Narell v Freeman* (9th Cir 1989) 872 F2d 907; *Worth v Selchow & Righter Co*. (9th Cir 1987) 827 F2d 569, cert denied (1988) 485 US 977. A compilation of facts, however, may be protected in part, to the extent that it features an original selection or arrangement, displaying some minimal level of creativity beyond mere collection of the data. *Feist,* 499 US at 358, 113 L Ed 2d at 377. See 17 USC §103. A compilation is defined as "a work formed by the collection and assembling of preexisting materials or of data that are selected, coordinated, or arranged in such a way that the resulting work as a whole constitutes an original work of authorship." 17 USC §101. For compilations, copyright protection extends "only to the material contributed by the author of such work, as distinguished from the preexisting material employed in the work." 17 USC §103(b). See *Assessment Technols. of WI, LLC v WIREData, Inc.* (7th Cir 2003) 350 F3d 640 (owner of copyrighted compilation could not prevent its customers from disclosing compiled data, which was in public domain). The same rule applies to derivative works, such as motion pictures based on novels, translations, reproductions, abridgements, recordings, and revisions. 17 USC §§101, 103(b).

The most significant feature of a copyrightable work is originality. "The mere fact that a work is copyrighted does not mean that every element of the work may be protected. Originality remains the sine qua non of copyright; accordingly, copyright protection may extend only to those components of a work that are original to the author." *Feist,* 499 US at 348, 113 L Ed 2d at 371. An Internet website is an example of a work composed of many different elements, not all of which will be protected by copyright law. See *Allen v Ghoulish Gallery* (SD Cal, Nov. 20, 2007, No. 06CV371 NLS) 2007 US Dist Lexis 86224, *13 (plaintiff may have copyright protection in selection, arrangement, and presentation of individual elements even if those elements did not qualify for protection individually).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/1 Copyrights and the DMCA/§1.3 C. Creation and Term of Copyright

§1.3 C. Creation and Term of Copyright

For works created on or after January 1, 1978, copyright protection begins at the time a work is created and continues, for works whose authors are individuals, for the life of the author plus 70 years—or, if the work is a "joint work" created by more than one author (see §1.4), the life of the last author to die plus 70 years. If the work is created as a "work made for hire" (defined in 17 USC §101; see §1.5), the copyright term will continue until the earlier of 95 years from first publication or 120 years from creation. 17 USC §302. For works created earlier than 1978, the rules for computing the term of the copyright are more complex. The U.S. Copyright Office has published a circular that explains how a term should be measured for pre-1978 works. See United States Copyright Office Circular 15a, available at http://www.copyright.gov/circs/circ15a.pdf.

Formerly, the term of a copyright was the author's lifetime plus 50 years. In 1998, Congress enacted the Sonny Bono Copyright Term Extension Act (CTEA) (Pub L 105-298, 112 Stat 2827) which extended the term to 70 years. 17 USC §302. A 2003 Supreme Court case rejected a challenge to Congress's power to extend the term of copyrights in existence before the effective date of the CTEA. *Eldred v Ashcroft* (2003) 537 US 186, 154 L Ed 2d 683, 123 S Ct 769.

NOTE: Section 514 of the Uruguay Round Agreements Act (Pub L 103-465, 108 Stat 4809, codified at 17 USC §§104A, 109) sets forth a procedure for restoring copyrights in works that have previously been in the public domain in the United States. Under §514, copyright protection under United States law is available for any work published almost anywhere in the world after 1923 if the original work was of qualified foreign, rather than United States, origin. In *Golan v Gonzales* (10th Cir 2007) 501 F3d 1179, the 10th Circuit held that §514's removal of works from the public domain altered the traditional contours of copyright protection and required scrutiny in light of the interests in free expression protected by the First Amendment. The court remanded the case with instructions for the district court to subject §514 to a First Amendment review.

© The Regents of the University of California

D. Ownership of Copyrighted Work, Joint Works, and Works Made for Hire

§1.4 1. Joint Works

Copyright vests initially in the author or authors of a work. 17 USC §201. If a work is created by more than one author, the work may be considered a "joint work." A joint work is defined as "a work prepared by two or more authors with the intention that their contributions be merged into inseparable or interdependent parts of a unitary whole." 17 USC §101. Each author of a joint work owns an undivided interest in the entire work and may license the entire work on a nonexclusive basis without obtaining consent from the co-author. Joint owners do, however, have a duty to account to each other for profits. See 17 USC §201, Notes ("co-owners of a copyright… treated generally as tenants in common, with each co-owner having an independent right to use or license the use of a work, subject to a duty of accounting to the other co-owners"). An assignment by a joint author may not exceed the extent of his or her ownership interest in the work, and the transferee becomes a co-tenant with the remaining joint author(s). *Donna v Dodd, Mead & Co.* (SD NY 1974) 374 F Supp 429.

© The Regents of the University of California

§1.5 2. Works Made for Hire

Although the general rule under §201 of the Copyright Act is that the person who creates a work is the "author" or owner of that work (see 17 USC §201(a)), there is an exception to that principle. Copyright law also defines a category of works called "works made for hire," and if a work is "made for hire," the employer, and not the employee (or, with respect to certain works described below, the commissioning party, and not the commissioned independent contractor), is considered the "author" or owner. 17 USC §201(b). The employer may be a firm, an organization, or an individual.

A "work made for hire" is defined as (17 USC §101):

> (1) a work prepared by an employee within the scope of his or her employment; or (2) a work specially ordered or commissioned for use as a contribution to a collective work, as a part of a motion picture or other audiovisual work, as a translation, as a supplementary work, as a compilation, as an instructional text, as a test, as answer material for a test, or as an atlas, if the parties expressly agree in a written instrument signed by them that the work shall be considered a work made for hire.

Whether a particular work is made for hire depends on the relationship between the parties. To determine whether a work is made for hire, one must first ascertain whether the work was prepared by an employee or an independent contractor. *Community for Creative Non-Violence v Reid* (1989) 490 US 730, 104 L Ed 2d 811, 109 S Ct 2166. If a work is created by an employee, the work will normally be considered a work made for hire. If a work is created by an independent contractor (that is, someone who is not an employee under the general common law of agency), then the work would have to qualify as a specially ordered or commissioned work, and subpart (2) of the statutory definition would apply. Such a work can be a work made for hire only if both of the following conditions are met: (a) It comes within one of the nine categories of works listed in subpart (2) of the definition, and (b) there is a written agreement between the parties specifying that the work is a work made for hire. 17 USC §101.

To help determine whether the creator of a work is an employee, the Supreme Court in *Reid* identified certain factors that characterize an employer-employee relationship as defined by agency law (490 US at 741, 104 L Ed 2d at 825):

- Control by the employer over the work (*e.g.,* the employer determines how the work is done, has the work done at the employer's location, and provides equipment or other means to create work);
- Control by the employer over the employee (*e.g.,* the employer controls the employee's schedule in creating work, has the right to have the employee perform other assignments, determines the method of payment, and has the right to hire the employee's assistants);
- Status and conduct of the employer (*e.g.,* the employer is in business to produce such works, provides the employee with benefits, and withholds tax from the employee's payment).

Note that these factors are not exhaustive, and the Court did not specify precisely which of these factors must be present to establish an employment relationship under the work-for-hire definition. The Court held, however, that supervision or control over creation of the work alone is not determinative. 490 US at 741, 104 L Ed 2d at 825. These factors characterize a regular, salaried employment relationship, and a work created within the scope of such employment is likely a work made for hire (unless the parties involved agree otherwise).

If a work is made for hire, the employer or other person for whom the work was prepared is the initial owner of the copyright unless both parties have signed a written agreement to the contrary. 17 USC §201(b).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/1 Copyrights and the DMCA/§1.6 E. Rights of Copyright Holder

§1.6 E. Rights of Copyright Holder

In general, a copyright owner has the following exclusive rights, and the right to authorize others to exercise the following rights, with respect to a work:

- The right to reproduce the work. 17 USC §106(1). See §§1.6A, 1.6C. This right precludes others from copying the work without permission.
- The right to prepare derivative works based upon the work. 17 USC §106(2). Under the Copyright Act, a "derivative work" is one based on "one or more preexisting works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which a work may be recast, transformed, or adapted." 17 USC §101.
- The right to distribute copies of the work to the public by sale or other transfer of ownership, or by rental, lease, or lending. 17 USC §106(3). See §1.6B. This right is limited by the "first sale doctrine," which states that after the first sale or distribution of a copy of a work, the copyright holder can no longer control further distribution of that copy. See §1.23. For example, if a book is purchased at a bookstore, that purchase is a "first sale" and the copyright holder cannot prevent the purchaser of the book from reselling it or renting it to others. 17 USC §109.
- The right to perform the work publicly, in the case of literary, musical, dramatic, and choreographic works, pantomimes, motion pictures, and other audiovisual works. 17 USC §106(4). See §1.6C. To perform or display a work publicly means "to perform or display it at a place open to the public or at any place where a substantial number of persons outside of a normal circle of a family and its social acquaintances is gathered," or to transmit it to multiple locations, such as through television or radio. 17 USC §101.
- The right to publicly display literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work. 17 USC §106(5).

These rights are limited statutorily in 17 USC §§107-121, including, *e.g.,* by the fair use doctrine as explained in §§1.18-1.22.

© The Regents of the University of California

§1.6A 1. Reproduction Rights

The law is developing with respect to the question of whether the right of reproduction is implicated when a computer program or other copyrighted material is copied to a computer's random access memory or buffer during routine operations. *MAI Sys. Corp. v Peak Computer, Inc.* (9th Cir 1993) 991 F2d 511, is widely cited for the proposition that temporary copies of a program stored in a computer's RAM can constitute an infringement of the copyright holder's reproduction right. In two more recent cases, courts have held that the reproduction right was not violated when the copies were less perceivable and existed for shorter durations than in *MAI*. In *Cartoon Network LP, LLLP v CSC Holdings, Inc.* (2d Cir 2008) 536 F3d 121, cert denied (2009) ___ US ___, 174 L Ed 2d 595, 129 S Ct 2890, a cable system's buffer retained a copy for no longer than 1.2 seconds, and in *CoStar Group, Inc. v. LoopNet, Inc.* (4th Cir 2004) 373 F3d 544, the copy was made by an Internet service provider acting as a conduit. In both cases, the court held that the copies were not "fixed" as defined at 17 USC §101 because they were not embodied "for a period of more than transitory duration." In any event, in the context of computer programs, 17 USC §117 provides important limitations on the exclusive rights set forth at 17 USC §106. See §1.16A.

© The Regents of the University of California

§1.6B 2. Distribution Rights

There is some question as to whether merely making a copyrighted work available to the public constitutes distribution under §106(3). One court has held that when a library makes unauthorized copies from its collection available to the public, it is sufficient to establish distribution for purposes of the statute. See *Hotaling v Church of Jesus Christ of Latter-Day Saints* (4th Cir 1997) 118 F3d 199. However, several courts have recently held that the mere act of making works available to the public in various online contexts, such as music file sharing, does not, by itself, necessarily constitute distribution. See *Perfect 10, Inc. v Amazon.com, Inc.* (9th Cir 2007) 508 F3d 1146; *Capitol Records, Inc. v Thomas* (D Minn 2008) 579 F Supp 2d 1210; *Atlantic Recording Corp. v Brennan* (D Conn 2008) 534 F Supp 2d 278; *Elektra Entertainment Group, Inc. v Barker* (SD NY 2008) 551 F Supp 2d 234.

© The Regents of the University of California

§1.6C 3. Performance Rights

Copyright law is unsettled with respect to the question of how Internet downloads implicate performance rights. In *U.S. v ASCAP* (SD NY 2007) 485 F Supp 2d 438, the court held that the act of downloading musical works via the Internet implicates the right of reproduction for purposes of determining royalty rates, but not the right of performance.

© The Regents of the University of California

§1.7 F. Copyright Notice

Copyright protection attaches when a work is fixed in a tangible medium of expression. 17 USC §102(a). Neither publication (with or without a copyright notice) nor registration is required under the Copyright Revision Act of 1976. See 17 USC §§401(a), 408(a). Because prior copyright law contained a notice requirement, however, the use of notice is still relevant to a determination of the copyright status of older works. See United States Copyright Office, Circular 3, available at http://www.copyright.gov/circs/circ03.pdf.

Although no longer required, use of a copyright notice may be important because it informs the public that the work is protected by copyright, identifies the copyright owner, and shows the year of first publication. Furthermore, affixing the notice may provide benefits in an infringement suit. If a proper notice of copyright appears on the published copy or copies to which a defendant in a copyright infringement suit had access, the defendant may not be able to pursue a defense based on "innocent infringement" in order to mitigate actual or statutory damages. See, *e.g.,* 17 USC §401(d) (when notice appears in form and position specified by §401, defendants generally not helped by claim of "innocent infringement").

"Innocent infringement" under the Copyright Act occurs when the infringer "was not aware and had no reason to believe that his or her acts constituted an infringement of copyright," and statutory damages for infringement may be reduced accordingly. 17 USC §504. See 17 USC §504, Notes. Innocent infringement protections also extend to "the special situation of teachers, librarians, archivists, and public broadcasters, and the nonprofit institutions of which they are a part," when a person or institution infringes copyrighted material honestly believing that its use constituted a "fair use." 17 USC §504(c)(2). See §§1.18-1.22. In this latter type of innocent infringement, when proven, a court is precluded from awarding any statutory damages.

The notice for visually perceptible copies of a work should contain each of the following three elements (17 USC §401(b)):

- The symbol © (the letter C in a circle), or the word "Copyright," or the abbreviation "Copr."; and
- The year of first publication of the work; and
- The name of the owner of copyright in the work, or an abbreviation by which the name can be recognized, or a generally known alternative designation of the owner. Example: ©2003 Jane Doe.

The notice must be affixed in such a manner and location as to give reasonable notice of the copyright claim. 17 USC §401(c); 37 CFR §201.20.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/1 Copyrights and the DMCA/ G. Copyright Registration/ §1.8 1. Advantages of Registration

G. Copyright Registration

§1.8 1. Advantages of Registration

Copyright registration is permissive and is not a condition of basic copyright protection under current law. 17 USC §408(a). Even though registration is not required, it provides the following advantages:

- Registration is a necessary prerequisite for a copyright infringement suit for works of U.S. origin. 17 USC §411(a).
- Registration establishes a public record of the copyright claim.
- If done before or within 5 years after the first publication of a work, registration will constitute prima facie evidence of the validity of the copyright and of the facts stated in the certificate of registration. 17 USC §410(c).
- If a work is registered within 3 months after first publication or in any event before an infringement occurs, statutory damages under 17 USC §504(c) and attorney fees may be recovered by the copyright owner. Otherwise, only actual damages would be recoverable by the copyright owner. 17 USC §412.
- Registration may allow the owner of the copyright to record the registration with the U.S. Customs Service for protection against the importation of infringing copies. For further information, see "How to Obtain Copyright, Trademark, and Patent Protection from the U.S. Customs Service," US Customs Service Brochure 563, available from the U.S. Customs Service, P.O. Box 7404, Washington, D.C. 20044, and http://www.customs.gov.

© The Regents of the University of California

§1.8A 2. Registration Procedures

Registration may be made at any time within the life of the copyright. The Copyright Office recommends that applicants for registration use its online system, the Electronic Copyright Office (eCO), a faster, less expensive procedure that enables online status tracking and the ability to upload certain types of electronic files directly. For further information concerning eCO, see http://www.copyright.gov/eco/index.html and http://www.copyright.gov/eco/tips.pdf. Additional information concerning copyright registration procedures is available at the Copyright Office website and in United States Copyright Office Circular 1, "Copyright Basics," available at http://www.copyright.gov/circs/circ01.pdf.

A nonrefundable filing fee and a nonreturnable deposit of the work being registered are also required for registration. Deposit requirements vary depending on the type of work involved. In general, the deposit requirement consists of two complete copies of the work. 17 USC §407(a)(1).

Computer software programs and databases are considered "literary works" for purposes of copyright registration. The graphic elements of a website, however, will fall into the "visual arts" category. If the work is an unpublished or published computer program, the deposit requirement consists of one visually perceptible copy in source code of the first 25 and last 25 pages of the program. For a program fewer than 50 pages in length, the deposit is a copy of the entire program. Additional deposit options are available for programs containing trade secrets: A deposit may be a portion of the source code that contains no trade secrets, or one that has had the trade secret portions blocked out. For more information on computer program registration, including deposits for revised programs and provisions for trade secrets, see United States Copyright Office Circular 61, "Copyright Registration for Computer Programs," available at http://www.copyright.gov/circs/circ61.pdf.

A copyright registration is effective on the date the Copyright Office receives all the required components in acceptable form, regardless of how long it then takes to process the application and mail the certificate of registration. 17 USC §410(d). Several courts outside the Ninth Circuit have held that a plaintiff copyright owner has standing to sue for infringement once the Copyright Office has received the owner's application, and that the owner does not need to wait for the certificate of registration. However, there is a circuit split on this issue. Compare *Goss Int'l Ams., Inc. v A-American Mach. & Assembly Co.* (ND Ill, Nov. 30, 2007, No. 07C3248) 2007 US Dist Lexis 88382 with *La Resolana Architects PA v Clay Realtors Angel Fire* (10th Cir 2005) 416 F3d 1195.

In *Moberg v 33T LLC* (D Del 2009) 666 F Supp 2d 415, the district court held that a work posted on a foreign website was not "published" in the United States for purposes of 17 USC §411 and therefore did not trigger the registration requirement.

© The Regents of the University of California

§1.8B 3. When to Register

As a practical matter, companies doing business online do not normally register each of their copyrights as a matter of course. For companies with software programs and websites that are in a state of constant revision and improvement, registration of each upgrade or modification can be expensive and time-consuming. Moreover, it can difficult to identify what parts of a work could be submitted for registration without disclosing any trade secrets. As a result, most technology companies only take steps to register works in connection with certain events—especially litigation, because registration must occur before an infringement suit can be filed. See 17 USC §411. Registration is also often required in connection with financings to enable the lender to take a security interest in the registered copyrights. See §16.27.

For companies requiring their partners or portfolio companies to register their copyrights, the registration requirement itself is likely only a first step. Thereafter, the company should ensure that subsequent versions and derivative works are also registered, and some oversight may be necessary to ensure that registrations do not unnecessarily disclose any confidential source code or other trade secrets.

© The Regents of the University of California

§1.8C H. Preregistration

The Artists' Rights and Theft Protection Act of 2005 (the ART Act) (Pub L 109-9, 119 Stat 218) provides for preregistration for certain works that are likely to face infringement while still in development. 17 USC §408(f). Preregistration entitles the owner of a work in progress to bring an infringement action before a work is commercially distributed. 17 USC §411(a). Only works that are "being prepared for commercial distribution" and can be categorized as "motion pictures, sound recordings, musical composition, literary works being prepared for publication in book form, computer programs (including videogames, advertising or marketing photographs)" are eligible. See the Copyright Office website at http://www.copyright.gov/prereg. Preregistration requires a $100 nonrefundable fee. Generally, preregistered works must be registered within 3 months of the publication of the work. 17 USC §408(f)(3).

© The Regents of the University of California

I. Transfer of Copyrights

§1.9 1. Generally

The Copyright Act defines a "transfer of copyright ownership" as (17 USC §101):

> an assignment, mortgage, exclusive license, or any other conveyance, alienation, or hypothecation of a copyright or of any of the exclusive rights comprised in a copyright, whether or not it is limited in time or place of effect, but not including an nonexclusive license.

Copyrights may be transferred in whole or in part by conveyance, by operation of law, or by bequest or devise. Any of the exclusive rights of a copyright holder specified in 17 USC §106 (see §1.6) may be transferred and held separately. 17 USC §201(d). Unless the transfer is by operation of law, all transfers of copyright ownership must be in writing and signed by the owner of the rights conveyed. 17 USC §204(a). The Copyright Office has a procedural guide for transferring copyrights. See United States Copyright Office Circular 12, available at http://www.copyright.gov/circs/circ12.pdf.

NOTE: The transfer rules in 17 USC §204 do not apply to nonexclusive licenses of copyrights. Nonexclusive licenses may be granted orally or even implied from conduct. *Lulirama Ltd, Inc. v Axcess Broad. Servs., Inc*. (5th Cir 1997) 128 F3d 872, 878.

Notarial acknowledgements are not required for validity, but constitute prima facie evidence of the execution of the transfer. 17 USC §204(b). The original or a certified copy of the transfer document may be recorded in the U.S. Copyright Office. A cover sheet as prescribed by the Copyright Office is required to be filed along with the transfer document. A copy of the cover sheet is reproduced in §1.11, and is available for downloading at http://www.copyright.gov/forms/formdoc.pdf. Recordation gives constructive notice to third parties of the transfer, provided that the work is registered and the document specifically identifies the work. 17 USC §205(a), (c). If there are two conflicting transfers, the one executed first prevails if it has been properly recorded within one month after execution in the United States (or within two months if executed outside the United States) or, in any event, before recordation of the later transfer. If the first executed transfer does not qualify, then the later transfer prevails if it is recorded first and if it has been taken in good faith for value and without notice of the first transfer. 17 USC §205(d). A nonexclusive license of a copyright (whether or not recorded) prevails over a conflicting transfer of ownership of the copyright if the license is reflected in a signed written instrument and if the license was taken either before the transfer or was taken in good faith before recordation of the transfer and without notice of it. 17 USC §205(e). Licenses and transfers are subject to termination as provided in 17 USC §203.

NOTE: By their terms, copyright licenses often prohibit transfers by the licensee without prior consent of the licensor. In *Cincom Sys., Inc. v Novelis Corp.* (6th Cir 2009) 581 F3d 431, the Sixth Circuit found that corporate merger and acquisition transactions may result in violations of non-transferable copyright licenses. The court held that the merger of two corporate subsidiaries as part of a corporate restructuring resulted in a transfer of a software license to the new corporate entity, thereby breaching the agreement's provision that the license could not be transferred without prior written approval.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/1 Copyrights and the DMCA/§1.10 2. Form: Copyright Assignment

§1.10 2. Form: Copyright Assignment

▶ To download **Word** version, right click and choose *Save Target As*

▶ To download **WordPerfect** version, right click and choose *Save Target As*

TRANSFER AND ASSIGNMENT OF COPYRIGHT

This Transfer and Assignment of Copyright (this "Assignment") is made and entered into as of _ _[*date*]_ _, by and between _ _[*name*]_ _ ("Assignor") and _ _[*name*]_ _ ("Assignee").

1. Assignor is the owner of the following copyrighted works (the "Works"):

[*Insert identifying information such as title and copyright registration, if any*]

2. For good and valuable consideration, the receipt of which is hereby acknowledged, Assignor hereby assigns, and transfers to Assignee, all of Assignor's interest in the Works and in the copyrights thereto, together with all rights to secure registrations, renewals, reissues, and extensions of the copyrights thereto.

3. Assignor hereby covenants, warrants, and represents to Assignee that:

(a) Assignor is the sole owner of and has the exclusive right to use the Works and the copyrights therein, free and clear of any liens, encumbrances, licenses, or claims of any nature, and has made no agreement with respect to the Works or the copyrights therein that is in conflict with this Agreement.

(b) Except as specified in Paragraph 1 of this Assignment, no other copyright has been effected, nor has any other registration relating to copyright protection been made with respect to the Works.

(c) If Assignor is an individual, Assignor agrees to authorize and direct his or her heirs and personal representatives to make and execute any instrument and perform any legal act that Assignee may deem necessary to secure the copyright, or any renewal or extension of the copyright to the Works.

4. This Assignment is governed by the laws of the State of California without regard to its conflict of law rules.

In witness whereof, the parties have executed this Assignment by their duly authorized representatives.

Assignor:

Date: _ _ _ _ _ _

_ _[*NAME OF ENTITY*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _
_ _[*Address*]_ _

Assignee:

Date: _ _ _ _ _ _

_ _[*NAME OF ENTITY*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _
_ _[*Address*]_ _

[*Insert Notarial Acknowledgment*]

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/1 Copyrights and the DMCA/§1.11 3. Form: U.S. Copyright Office Cover Sheet

§1.11 3. Form: U.S. Copyright Office Cover Sheet



Document Cover Sheet

UNITED STATES COPYRIGHT OFFICE

Copyright Office fees are subject to change.
For current fees check the Copyright Office website at *www.copyright.gov*, write to the Copyright Office, or call (202) 707-3000.

For Recordation of Documents

Volume _____ Document _____

Volume _____ Document _____

Date of recordation M _____ D _____ Y _____
(ASSIGNED BY THE COPYRIGHT OFFICE)

Funds received _____

DO NOT WRITE ABOVE THIS LINE · SEE INSTRUCTIONS ON REVERSE

To the Register of Copyrights: *Please record the accompanying original document or properly certified copy thereof.*

1 First party name given in the document _____
(IMPORTANT: *Please read instruction for this and other spaces.*)

2 First title given in the document _____

3 Total number of titles in the document _____

4 Amount of fee calculated _____

5 Fee enclosed

☐ Check ☐ Money order
☐ Fee authorized to be charged to Copyright Office deposit account

Deposit account number _____

Deposit account name _____

6 Completeness of document

☐ Document is complete by its own terms ☐ Document is not complete. Record "as is."

IMPORTANT NOTE: *A request to record a document "as is" under 37 CFR §201.4(c)(2) is an assertion that: (a) the attachment is completely unavailable for recordation; (b) the attachment is not essential to the identification of the subject matter of the document; and (c) it would be impossible or wholly impracticable to have the parties to the document sign or initial a deletion of the reference to the attachment.*

7 Certification of Photocopied Document

Complete this certification if a photocopy of the original signed document is substituted for a document bearing the actual original signature.
NOTE: *This space* may not *be used for documents that require an official certification.*

I declare under penalty of perjury that the accompanying document is a true and correct copy of the original document.

Signature _____ Date _____

Duly authorized agent of _____

8 Return to:

Name _____

Number/street _____ Apt/suite _____

City _____ State _____ Zip _____

Phone number _____ Fax number _____

Email _____

SEND TO: *Library of Congress, Copyright Office, Documents Recordation Section, 101 Independence Avenue SE, Washington, DC 20559-6000*
INCLUDE ALL THESE TOGETHER: (1) Two copies of this form; (2) payment from a deposit account or by check/money order payable to *Register of Copyrights*; and (3) your document.

FORM DCS REV: 09/2007 PRINT: 09/2007—••,000 Printed on recycled paper U.S. Government Printing Office: 2007-330-945/60,•••

Print

Document Cover Sheet · Basic Information

Read all of the instructions below before completing this form. Use of the Document Cover Sheet is optional but encouraged.

When to use this form Use the Document Cover Sheet when you are submitting a document for recordation in the U.S. Copyright Office.

Mailing requirements It is important to send the original cover sheet and one copy of the cover sheet for each document that is being submitted for recordation. The two copies of the Document Cover Sheet, the document, and the fee must be sent together in the same envelope or package. The Copyright Office cannot process them unless they are received together. Send to: *Library of Congress, Copyright Office, Documents Recordation Section, 101 Independence Avenue SE, Washington, DC 20559-6000*

Cover sheets should be typed or printed and should contain the information requested so that the Copyright Office can process the document and return it. Be sure to complete space 8 so that the recorded document can be returned. The Copyright Office will process the document based on the information in the document or an attachment that is part of the document. Information for indexing will not be taken from the Document Cover Sheet or attachments that were *not* part of the document when it was executed (signed). To be recorded, the document must satisfy the recordation requirements of the copyright law and Copyright Office regulations.

The person submitting a document with a cover sheet is solely responsible for verifying the correctness of the cover sheet and the sufficiency of the document. Recording a document submitted with or without a cover sheet does not constitute a determination by the Copyright Office of the document's validity or effect. Only a court may make such a determination.

When a Document Cover Sheet is submitted, it will be imaged with the document as part of the public record.

PRIVACY ACT ADVISORY STATEMENT (*Required by the Privacy Act of 1974 (P.L. 93-579)*): The authority for requesting this information is title 17 *USC*, sec. 205. Furnishing the requested information is voluntary. But if the information is not provided, it may be necessary to delay recordation.

The principal uses of the requested information are the establishment and maintenance of a public record and the evaluation for compliance with the recordation requirements of section 205 of the copyright code. Other routine uses include public inspection and copying, preparation of public indexes, preparation of public catalogs of copyright recordations, and preparation of search reports upon request.

NOTE: No other advisory statement will be given in connection with this application. Please keep this statement and refer to it if we communicate with you regarding this cover sheet.

Space-by-Space Instructions

Space 1: First party given in the document This information is only used to connect the Document Cover Sheet and the document if they become separated. No information is entered in the catalog record from this space.

Space 2: First title given in the document This information is only used to connect the Document Cover Sheet and the document if they become separated. No information is entered in the catalog record from this space.

Space 3: Total number of titles in the document The total number of titles (including a.k.a. and other variant titles of a work) determines the recordation fee. In the case of multiple title documents, titles that are repeated in documents are counted as a single title, except where the document lists different issues, volumes, episode numbers, etc. following each title. Each such entry is regarded as a separate title and will be indexed separately and counted separately when computing the fee for recording the document. The Copyright Office verifies title counts.

Space 4: Amount of fee calculated There is a basic fee for recording a document containing one title. There is an additional charge for each group of up to 10 additional titles. "Alternative" titles, "formerly-known-as" titles, and "also-known-as" titles are considered to be extra titles. Titles are counted by groups. If there are fewer than 10 titles in a group, the fee for a group still applies. Copyright Office fees are subject to change. For current fees, check the Copyright Office website at *www.copyright.gov*, write the Copyright Office, or call (202) 707-3000. Please remember that the fee is based on the number of titles in a document, not the number of works.

Space 5: Fee enclosed Check the appropriate box. If a Copyright Office deposit account is to be charged, give the Copyright Office deposit account number and name. The Office only accepts domestic money orders and checks payable through a U.S. bank with American Bankers Association routing numbers. International and postal money orders are not accepted.

Space 6: Completeness of document Check the appropriate box. Please read the "Important note"if checking "Record 'as is.'"All documents recorded under §205 of the Copyright Act must be complete by their own terms to be recorded. Notices of termination recorded under §203, §304(c), and §304(d) must be complete and exact duplicates of the notices as served. Please refer to Copyright Office regulations in Chapter 37 *CFR* §201.4 and §201.10 and Circular 12, *Recordation of Transfers and Other Documents*, for more information.

Space 7: Certification of photocopied documents Complete this section only if submitting a photocopied document in lieu of a document bearing the actual original signature. If a photocopy of the original signed document is submitted, it must be accompanied by a sworn certification. A sworn certification signed by at least one of the parties to the document or that party's authorized representative (who is identified as such at space 7) will satisfy that requirement. The date entered in the date field should be the date you sign the Document Cover Sheet. Copies of documents on file in a federal, state, or local government office must be accompanied by an original official certification.

Space 8: Return to Give the name and address of the person to whom the recorded document should be returned. The Copyright Office does not maintain paper files of recorded documents. The documents are imaged and returned to the person or firm designated in this space. Please include telephone number, fax number, and email address in case we need to contact you.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/1 Copyrights and the DMCA/ J. Infringement/§1.12 1. Generally

J. Infringement

§1.12 1. Generally

Anyone who violates any of the exclusive rights of the copyright owner without permission falls within the definition of an infringer under the Copyright Act. 17 USC §501. In the Ninth Circuit, a plaintiff establishes a prima facie case of direct copyright infringement by showing (*A&M Records, Inc. v Napster, Inc*. (9th Cir 2001) 239 F3d 1004, 1013; *Narell v Freeman* (9th Cir 1989) 872 F2d 907, 910):

- The plaintiff's ownership of the copyright;
- The defendant's copying of protected elements of the work (or other violation of one of the plaintiff's exclusive rights as a copyright holder granted by 17 USC §106).

See also *Brown Bag Software v Symantec Corp*. (9th Cir 1992) 960 F2d 1465, cert denied (1992) 506 US 869. In most cases, direct evidence of copying will not be available. Therefore, a plaintiff may establish copying by showing that (1) the infringer had access to the work and (2) the two works are substantially similar. *Narell v Freeman*, 872 F2d at 910. To show substantial similarity, the Ninth Circuit employs a two-part test (*Apple Computer, Inc. v Microsoft Corp*. (9th Cir 1994) 35 F3d 1435, 1442, cert denied (1995) 513 US 1184):

- An objective, extrinsic test, which determines whether the two works at issue are substantially similar in ideas and expression and compares the individual elements of the works to find specific similarities between them; and
- A subjective, intrinsic test, which determines whether the forms of expression of the two works are substantially similar, based on the viewpoint of an ordinary and reasonable observer. "To constitute infringement, the total concept and feel of the works must be substantially similar." *Narell v Freeman* (9th Cir 1989) 872 F2d 907, 913.

See also *Metcalf v Bochco* (9th Cir 2002) 294 F3d 1069; *Shaw v Lindheim* (9th Cir 1990) 919 F2d 1353; *Berkic v Crichton* (9th Cir 1985) 761 F2d 1289, cert denied (1985) 474 US 826. In applying the extrinsic test to compare the expression of ideas embodied in two software programs, the court will engage in a process of "analytical dissection," comparing screens, menus, and keystrokes. *Brown Bag Software,* 960 F2d at 1475. A graphical user interface will be analyzed as an artistic, audiovisual work, rather than as program codes registered as a literary work. *Apple Computer, Inc. v Microsoft Corp*. (9th Cir 1994) 35 F3d 1435, 1439, cert denied (1995) 513 US 1184. Analytical dissection is also relevant to an analysis of the copyrightability of the work and the scope of the copyright. *Brown Bag Software,* 960 F2d at 1476.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/1 Copyrights and the DMCA/ 2. Direct, Contributory, and Vicarious Liability/§1.13 a. Generally

2. Direct, Contributory, and Vicarious Liability

§1.13 a. Generally

A suit for copyright infringement can be brought against "direct infringers," "contributory infringers," or "vicarious infringers." See *Fonovisa, Inc. v Cherry Auction, Inc*. (9th Cir 1996) 76 F3d 259, 261; *Fonovisa, Inc. v Napster, Inc*. (ND Cal, Jan. 28, 2002) 2002 US Dist Lexis 4270. A direct infringer is recognized in the Copyright Act as any person or entity who exercises one of the exclusive rights of the copyright holder without permission. 17 USC §501. See §1.6. Contributory infringement is based on tort law and is an outgrowth of enterprise liability. A contributory infringer is someone who, with knowledge of the infringement, induces, causes, or materially contributes to the infringing conduct of another person or entity. *A&M Records, Inc. v Napster, Inc*. (9th Cir 2001) 239 F3d 1004, 1019; *Fonovisa, Inc. v Cherry Auction, Inc*. (9th Cir 1996) 76 F3d 259, 264. A vicarious infringer is someone who has the right and ability to supervise or control the acts of the direct infringer and also has a direct financial interest in the infringing act. Vicarious infringement may be shown even in the absence of an employer-employee relationship. 76 F3d at 262. See also *Gershwin Publ. Corp. v Columbia Artist Mgmt., Inc*. (2d Cir 1971) 443 F2d 1159, 1162; *Shapiro, Bernstein & Co. v H.L. Green Co.* (2d Cir 1963) 316 F2d 304.

NOTE: These distinctions are highly fact-based and subject to interpretation. Much of the Internet-related case law in this area concerns the liability of Internet service providers (ISPs), bulletin board service (BBS) operators, and other providers of online products or services, based on the infringing activities of their users. See, *e.g., Perfect 10, Inc. v Visa Int'l Serv. Ass'n* (9th Cir 2007) 494 F3d 788, cert denied (2008) ___ US ___, 171 L Ed 2d 811, 128 S Ct 2871; *Ellison v Robertson* (9th Cir 2004) 357 F3d 1072; *A&M Records, Inc. v Napster, Inc*. (9th Cir 2001) 239 F3d 1004.

© The Regents of the University of California

§1.14 b. Direct Infringement

To establish direct infringement liability by an ISP or BBS for infringing postings and unauthorized uses by users, there must be a direct volitional act on the part of the service provider. *Religious Technol. Ctr. v Netcom On-Line Communication Servs., Inc.* (ND Cal 1995) 907 F Supp 1361, 1381 (no ISP liability for direct infringement absent allegations that defendant affirmatively caused infringing copies to be made); *Playboy Enters., Inc. v Russ Hardenburgh, Inc.* (ND Ohio 1997) 982 F Supp 503, 512 (necessary volition existed when defendant provider established incentive program giving users "credit" for photographs they uploaded and defendant's employees viewed and organized uploaded materials). See also *CoStar Group, Inc. v LoopNet, Inc.* (4th Cir 2004) 373 F3d 544 (service provider's cursory review of copyrighted real estate photographs did not provide volitional element required for direct infringement claim).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/1 Copyrights and the DMCA/§1.15 c. Contributory Infringement

§1.15 c. Contributory Infringement

To establish contributory infringement, actual or constructive knowledge by the defendant of the direct infringement by third parties is required. *A&M Records, Inc. v Napster, Inc*. (9th Cir 2001) 239 F3d 1004, 1020. See also *Fonovisa, Inc. v Napster, Inc*. (ND Cal, Jan. 28, 2002) 2002 US Dist Lexis 4270. In many instances, an ISP or BBS serves merely as a passive information conduit and has no actual knowledge of the infringement. However, once an ISP or BBS knows or has reason to know of the direct infringement (for example, through complaints from the copyright holder or information gleaned by monitoring its system), the system provider may have met the contributory infringement standard. In *Perfect 10, Inc. v Amazon.com, Inc.* (9th Cir 2007) 508 F3d 1146, 1172, the Ninth Circuit found that defendant Google could be held contributorily liable if it "'has actual knowledge that specific infringing material is available using its system,'… and can 'take simple measures to prevent further damage' to copyrighted works … yet continues to provide access to infringing works."

In *A&M Records, Inc. v Napster, Inc*. (9th Cir 2001) 239 F3d 1004, the Ninth Circuit affirmed the district court's conclusion that knowledge of specific acts of infringement is not required for contributory liability. Napster was found to have constructive knowledge because its executives had experience in the recording industry, had enforced intellectual property rights in other contexts, had themselves downloaded copyrighted songs from Napster's system, and had promoted the site using lists of infringing files. 239 F3d at 1020 n5.

In *Religious Technol. Ctr. v Netcom On-Line Communication Servs., Inc.* (ND Cal 1995) 907 F Supp 1361, 1368, the district court refused to hold Netcom, an ISP, directly liable for an automatic pass-through of allegedly infringing messages posted by a subscriber, because Netcom performed no volitional act to facilitate the infringement. Netcom could be liable for contributory infringement, however, because it participated substantially in the public distribution of the infringing message by failing to delete it and thereby stop an infringing copy from being distributed. 907 F Supp at 1374. The court noted that if an ISP is unable to verify infringement—either because of a potential fair use defense, the absence of copyright notices, or the copyright owner's failure to provide necessary documentation to show the likelihood of infringement—there would be no contributory liability because the ISP's lack of knowledge would be reasonable. 907 F Supp at 1374.

An ISP or BBS that encourages or facilitates subscribers' infringing activities may be held liable for contributory infringement. See *Sega Enters. Ltd. v MAPHIA* (ND Cal 1996) 948 F Supp 923, 933 (BBS operator had knowledge of infringing activity and had specifically solicited and encouraged BBS users to upload and download plaintiff's video games); *Sega Enters. Ltd. v Sabella* (ND Cal, Dec. 18, 1996, No. C 93-04260 CW) 1996 US Dist Lexis 20470 (BBS operator advertised copiers that enabled subscribers to copy plaintiff's games); *Playboy Enters., Inc. v Webbworld, Inc.* (ND Tex 1997) 968 F Supp 1171, aff'd without opinion (5th Cir 1999) 168 F3d 486 (defendant had some control over materials distributed over its site and based its business model on commerce in images, not mere access to Internet). See also *Arista Records, Inc. v MP3Board, Inc.* (SD NY, Aug. 29, 2002) 2002 US Dist Lexis 16165 (triable issue of material contribution to direct infringement existed when service provider hosted automated system and message board devoted to searching out songs sought by users).

© The Regents of the University of California

§1.16 d. Vicarious Infringement

The doctrine of vicarious infringement is an outgrowth of the agency principle of respondeat superior. A vicarious infringer is one who has the right and ability to control the acts of the direct infringer and has a direct financial interest in the infringing act. *Fonovisa, Inc. v Cherry Auction, Inc*. (9th Cir 1996) 76 F3d 259, 262, citing *Gershwin Publ. Corp. v Columbia Artist Mgmt., Inc*. (2d Cir 1971) 443 F2d 1159, 1162. See also *Shapiro, Bernstein & Co. v H.L. Green Co.* (2d Cir 1963) 316 F2d 304, 307 (store owner who possessed "right and ability to supervise" infringing concessionaire and who received percentage of concessionaire's profits was vicariously liable for infringing activity, even without actual knowledge of the infringement). See also *Perfect 10, Inc. v Amazon.com, Inc.* (9th Cir 2007) 508 F3d 1146, 1174 (vicarious liability claim unlikely to succeed because defendant lacked "practical ability to police the infringing activities of third-party websites").

A finding of vicarious liability requires more than the act of manufacturing and distributing a product that consumers might use for infringing purposes. In *Sony Corp. v Universal City Studios, Inc*. (1984) 464 US 417, 78 L Ed 2d 574, 104 S Ct 774, the Court held that although a video recorder could be used to infringe on the rights of copyright holders, the mere sale of the device, which was used primarily for non-infringing purposes, did not establish vicarious liability. The *Sony* Court stated (464 US at 439, 78 L Ed 2d at 590):

> If vicarious liability is to be imposed on [Sony] in this case, it must rest on the fact that they have sold equipment with constructive knowledge of the fact that their customers may use that equipment to make unauthorized copies of copyrighted material. There is no precedent in the law of copyright for the imposition of vicarious liability on such a theory.

The defendant's actual knowledge of infringing activities and its ability to police those activities suggested that the plaintiff was likely to succeed on claims of contributory and vicarious liability in *A&M Records, Inc. v Napster, Inc.* (9th Cir 2001) 239 F3d 1004. The court found that "Napster had the right and ability to police its system and failed to exercise that right to prevent the exchange of copyrighted material." 239 F3d at 1022.

By contrast, in the Ninth Circuit's (now overturned) ruling in *Metro-Goldwyn-Mayer Studios, Inc. v Grokster, Ltd.* (9th Cir 2004) 380 F3d 1154, vacated and remanded (2005) 545 US 913, the appellate court had agreed with the district court that, "unlike Napster, [the defendants] do not operate and design an 'integrated service,' [citation] which they monitor and control." 380 F3d at 1165. More generally, the court found that "[t]he sort of monitoring and supervisory relationship that has supported vicarious liability in the past is completely absent in this case." 380 F3d at 1165. In 2005, in reversing the Ninth Circuit, the Supreme Court declined to rule on the application of a theory of vicarious liability to *Grokster*, acknowledging that the plaintiff-appellants had advanced such a theory, but "[b]ecause we resolve the case based on an inducement theory, there is no need to analyze separately MGM's vicarious liability theory." 545 US at 931 n9, 162 L Ed 2d at 797 n9.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/1 Copyrights and the DMCA/§1.16A e. Inducement

§1.16A e. Inducement

In *Metro-Goldwyn-Mayer Studios, Inc. v Grokster, Ltd.* (2005) 545 US 913, 162 L Ed 2d 781, 125 S Ct 2764, a unanimous United States Supreme Court reversed a ruling of the Ninth Circuit and held that the respondents, distributors of peer-to-peer, file-sharing computer networking software, could be held liable for acts of infringement by the users of that software. Although the Supreme Court had been widely expected to use *Grokster* to reexamine the "substantial noninfringing uses" test from *Sony,* the Court ultimately did not have a majority that could agree on how *Sony* (see §1.16) should be applied to the facts of *Grokster*. Instead, the Court held that (162 L Ed 2d at 799):

> where evidence goes beyond a product's characteristics or the knowledge that it may be put to infringing uses, and shows statements or actions directed to promoting infringement, *Sony*'s staple-article rule will not preclude liability.

The Court articulated a new doctrine of indirect copyright infringement liability by "inducement," holding that it is possible to "infringe contributorily by intentionally inducing or encouraging direct infringement." 162 L Ed 2d at 796. The inducement rule adopted by the Court provides the following (162 L Ed 2d at 800):

> [O]ne who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.… The inducement rule … premises liability on purposeful, culpable expression and conduct, and thus does nothing to compromise legitimate commerce or discourage innovation having a lawful promise.

The Court further explained that "[t]he classic instance of inducement is by advertisement or solicitation that broadcasts a message designed to stimulate others to commit violations." 162 L Ed 2d at 802.

In *Grokster,* the Court found the record "replete with evidence" that each of the defendants "clearly voiced the objective that recipients use [the software] to download copyrighted works, and each took active steps to encourage infringement" (162 L Ed 2d at 792), and found "substantial evidence" in favor of plaintiff-petitioners "on all elements of inducement," remanding the case to the district court to reconsider plaintiff-petitioners' motion for summary judgment (162 L Ed 2d at 803). On the *Grokster* Court's decision to forgo analysis of vicarious infringement, see §1.16.

Grokster, with its new articulation of secondary liability for inducement of infringement, was quickly hailed by some experts and criticized by others. See Peters, *Statement: Protecting Copyright and Innovation in a Post-Grokster World* (Sept. 28, 2005), U.S. Senate Committee on the Judiciary (praising *Grokster* as "sufficiently flexible to withstand the test of time and evolution of technology" and likely to have many positive permanent effects); but see von Lohmann, *Remedying 'Grokster'* (July 25, 2005), available at http://www.eff.org/deeplinks/2005/07/remedying-i-grokster-i (describing technology lawyers' frustration in the wake of *Grokster*, which creates "a dangerous minefield of legal uncertainties"). One of the first courts to incorporate *Grokster* into its analysis ultimately found that the defendant was not liable for inducing copyright infringement. See *Monotype Imaging, Inc. v Bitstream Inc.* (ND IL 2005) 376 F Supp 2d 877, 889 ("Bitstream did not have knowledge of plaintiffs' infringement, let alone act with the 'purposeful, culpable expression and conduct' that the Supreme Court found present in the *Grokster* defendants' conduct"). See also *Perfect 10, Inc. v Visa Int'l Serv. Ass'n* (9th Cir 2007) 494 F3d 788, 802 (rejecting inducement claim when plaintiff did not allege any "'specific acts' intended to encourage or induce infringement" (quoting *Grokster*)).

The precise contours of *Grokster*'s inducement test are continuing to emerge as additional courts have the opportunity to interpret and apply *Grokster,* particularly in cases where the facts are ambiguous as to the defendants' conduct and intent.

© The Regents of the University of California

§1.16B 3. Safe Harbor for Certain Copies of Computer Programs

Under the Copyright Act, the owner of a copy of a computer program may make an additional copy or adapt the program under certain conditions without infringing the copyright of the owner of the program. 17 USC §117(a). Section 117 also provides a safe harbor for software owners and lessees to copy a program for purposes of maintenance or repair if the copy is made "by virtue of the activation of the machine" and if it is destroyed immediately after the machine is serviced. 17 USC §117(c). See *Storage Technol. Corp. v Custom Hardware Eng'g & Consulting, Inc.* (Fed Cir 2005) 421 F3d 1307, 1314 (defendants' use of plaintiff's maintenance code, which was "so entangled with the functional code that the entire code must be loaded into RAM for the machine to function at all," did not violate copyright law).

The distinction between a software license and the sale of software is important in the §117 context because the safe harbor applies only to the owner of a copy of the computer program. In *Wall Data Inc. v Los Angeles County Sheriff's Dep't* (9th Cir 2006) 447 F3d 769, the court held that the purchaser of a copy of a software program is a licensee and not an owner of the copy if the copyright holder has made clear that a license is being granted, and the use or transfer of the copy is severely restricted, and that the defense under §117 is therefore not available. See also *Triad Sys. Corp. v Southeastern Express Co.* (9th Cir 1995) 64 F3d 1330, 1333; *MAI Sys. Corp. v Peak Computer, Inc.* (9th Cir 1993) 991 F2d 511. But see *Vernor v Autodesk, Inc.* (WD Wash 2009) 93 USPQ2d 1336, in which the district court interpreted the difference between an owner and a licensee based on the earlier precedent set by *U.S. v Wise* (9th Cir 1977) 550 F2d 1180. The court rejected as irreconcilable the conflicting reasoning of *Wall Data*, *Triad*, and *MAI*, none of which cited *Wise*.

© The Regents of the University of California

§1.17 4. Remedies

Remedies for infringement include injunctive relief (17 USC §502), impounding and destruction of the infringing article (17 USC §503), and recovery of actual damages, along with any profits of the infringer attributable to the infringement that are not taken into account in computing actual damages (17 USC §504). If the work was registered within three months of its publication, the copyright holder may recover statutory damages of up to $150,000 for each willful infringement or up to $30,000 per infringement if the infringement was not willful. 17 USC §504. A court may also, in its discretion, award attorney fees and costs. 17 USC §505. Common law punitive damages are not available under the Act. *Viacom Int'l, Inc. v YouTube, Inc.* (SD NY 2008) 540 F Supp 2d 461.

The Copyright Act establishes criminal liability for any person who willfully infringes a copyright "(1) for purposes of commercial advantage or private financial gain, or (2) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies … of 1 or more copyrighted works, which have a total retail value of more than $1,000." 17 USC §506(a). The penalty for violation is set forth in 18 USC §2319, which provides for monetary fines as well as prison terms of up to 10 years, depending on the dollar value of the infringement and the number of offenses the infringer has engaged in. In addition, the court may order the forfeiture and destruction of infringing copies and all devices or equipment used in their manufacture. 17 USC §506(b).

In October 2008, Congress enacted the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO-IP Act) (Pub L 110-403, §3, 122 Stat 4257), which, among other things, enhances certain penalties for violation of civil and criminal intellectual property laws; prohibits exportation (in addition to importation under current law) of infringing copies of copyrighted works; includes additional civil and criminal forfeiture provisions; and amends federal sentencing guidelines for the exportation of infringing materials.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/1 Copyrights and the DMCA/ K. Fair Use/§1.18 1. Introduction

K. Fair Use

§1.18 1. Introduction

The exclusive rights of a copyright holder are subject to certain limitations found in §§107-122 of the Copyright Act. Perhaps the most important of these limitations is the "fair use" doctrine, which developed judicially but is now codified in 17 USC §107. Section 107 provides that the "fair use" of a work for purposes such as "criticism, comment, news reporting, teaching … scholarship or research" does not constitute copyright infringement, and sets out four factors to be considered in determining whether or not a particular use is "fair":

> (1) the purpose and character of the use, including whether such use is of commercial nature or is for nonprofit educational purposes;
> (2) the nature of the copyrighted work;
> (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
> (4) the effect of the use upon the potential market for or value of the copyrighted work.

These factors are not exhaustive, and others may be relevant to the issue. See *Harper & Row, Publishers, Inc. v Nation Enters.* (1985) 471 US 539, 85 L Ed 2d 588, 105 S Ct 2218 (fact that defendant's infringing article was "news," one of §107's enumerated examples of fair use, did not preclude finding of copyright infringement); 4-13 Nimmer on Copyright §13.05[A]. The H Comm of the Judiciary, 87th Cong, 1st Sess (1961), Report of the Register of Copyrights on the General Revision of the U.S. Copyright Law, gives examples of activities that courts have regarded as fair use:

- Quotation of excerpts in a review or criticism for purposes of illustration or comment;
- Quotation of short passages in a scholarly or technical work, for illustration or clarification of the author's observations;
- Use in a parody of some of the content of the work parodied;
- Summary of an address or article, with brief quotations, in a news report;
- Reproduction by a library of a portion of a work to replace part of a damaged copy; reproduction by a teacher or student of a small part of a work to illustrate a lesson; reproduction of a work in legislative or judicial proceedings or reports; and
- Incidental and fortuitous reproduction, in a newsreel or broadcast, of a work located in the scene of an event being reported.

Whether a specific use constitutes a "fair use" or an infringement is not subject to a bright-line analysis, and requires a case-by-case approach. There is no specific number of words, lines, or notes that may safely be taken without permission. The fair use doctrine is an "equitable rule of reason." *Sony Corp. v Universal City Studios, Inc*. (1984) 464 US 417, 448, 78 L Ed 2d 574, 596, 104 S Ct 774. It provides flexibility in the law, which "permits courts to avoid rigid application of the copyright statute when, on occasion, it would stifle the very creativity which that law is designed to foster." *Iowa State Univ. Research Found., Inc. v American Broad. Cos.* (2d Cir 1980) 621 F2d 57, 60. When undertaking an analysis of the applicability of the fair use doctrine in any specific instance, counsel should review the case law interpreting each element listed in 17 USC §107 (see §§1.19-1.22) and bear in mind the difficulty of making definitive judgments in this area. See generally Spoo, *Fair Use in the Digital Age*, 23 CEB Cal Bus L Prac (Spring 2008).

NOTE: Acknowledging the source of copyrighted material (*e.g.,* citing or otherwise appropriately referencing the attribution of text or images) does not create a fair use or substitute for obtaining permission from the copyright owner. Often clients mistakenly believe that as long as copied text or images are properly footnoted so that attribution is correctly given to another, they have no liability. This is not the case. Absent fair use or another exemption from infringement, consent must be obtained from the copyright owner. When in doubt, permission should be obtained. See chap 14 on obtaining consent to use, and licensing, content for an Internet website. Note, however, that to seek permission in good faith generally does not preclude or undermine a fair use defense.

© The Regents of the University of California

§1.19 2. Purpose and Character of Use

Each of the four factors listed in 17 USC §107 (see §1.18) must be considered in analyzing whether a particular nonconsented use of copyrighted material is fair; no single factor is dispositive. *Campbell v Acuff-Rose Music, Inc*. (1994) 510 US 569, 578, 127 L Ed 2d 500, 515, 114 S Ct 1164. Thus, each factor has been subject to extensive judicial analysis and interpretation. See, *e.g., A&M Records, Inc. v Napster, Inc.* (9th Cir 2001) 239 F3d 1004; *Worldwide Church of God v Philadelphia Church of God, Inc.* (9th Cir 2000) 227 F3d 1110, 1117, cert denied (2001) 532 US 958; *Religious Technol. Ctr. v Netcom On-Line Communication Servs., Inc*. (ND Cal 1995) 923 F Supp 1231, 1243.

The first factor requires the court to review the purpose and character of the use, including, in particular, whether the use is commercial or instead is for nonprofit educational purposes. 17 USC §107(1). The focus of this inquiry is whether the allegedly infringing work "merely 'supersedes the objects' of the original creation… or instead adds something new, with a further purpose or different character, altering the first with new expression, meaning, or message;… whether and to what extent the new work is 'transformative.'" *Campbell v Acuff-Rose Music, Inc*. (1994) 510 US 569, 579, 127 L Ed 2d 500, 516, 114 S Ct 1164. The commercial or educational character of the use is only one element of this analysis. The fact that a use is commercial weighs against fair use, but a noncommercial use is not insulated from a finding of infringement. 510 US at 584, 127 L Ed 2d at 519. If the use of the new work is for the same essential purpose as the original work, the use is not likely to be deemed a fair use. *Worldwide Church of God v Philadelphia Church of God, Inc*. (9th Cir 2000) 227 F3d 1110, 1117, cert denied (2001) 532 US 958.

Two courts of appeal have held that copying and disassembling the object code of a computer program in connection with reverse engineering is a fair use, provided that the purpose is to understand the ideas in the program and that the final work produced through reverse engineering is not substantially similar to the work that is reverse-engineered. *Atari Games Corp. v Nintendo of Am., Inc.* (Fed Cir 1992) 975 F2d 832, 842. See also *Atari Computer Entertainment Am., Inc. v Bleem, LLC* (9th Cir 2000) 214 F3d 1022 (use of copyrighted "screen shots" in advertising for video game emulator was fair use); *Sega Enters. Ltd. v Accolade, Inc.* (9th Cir 1992) 977 F2d 1510.

In *Kelly v Arriba Soft Corp.* (9th Cir 2003) 336 F3d 811, the copying and storage of low-resolution thumbnail images of copyrighted photographs by an Internet search engine was held to be a fair use because it was done for the purpose of helping index and improve access to images on the Internet. This use was different from the illustrative and aesthetic purpose of the original photographs, and was therefore considered "transformative." Following *Arriba* in *Perfect 10, Inc. v Amazon.com, Inc.* (9th Cir 2007) 508 F3d 1146, the Ninth Circuit found Google's indexing of Perfect 10's thumbnail images a sufficiently transformative use to outweigh any commercial benefit Google might realize. See also *Ticketmaster LLC v RMG Technols., Inc.* (CD Cal 2007) 507 F Supp 2d 1096, 1105 (copies of web pages automatically cached upon viewing are within the Copyright Act's definition of copy); *Parker v Google* (Ed Pa 2006) 422 F Supp 2d 492, 497, aff'd (3d Cir 2007) 242 Fed Appx 833, cert denied (2008) ___ US ___, 169 L Ed 2d 834, 128 S Ct 1101 (automatic archiving of USENET postings and website excerpts in response to search queries does not constitute direct infringement); *Field v Google, Inc.* (D Nev 2006) 412 F Supp 2d 1106 (availability of "cached" links to plaintiff's copyrighted works from defendant's search engine held to be fair use of those copyrighted works; defendant entitled to protection of system caching safe harbor (17 USC §512(b), discussed in §1.32 below)).

© The Regents of the University of California

§1.20 3. Nature of Copyrighted Work

The second factor (see 17 USC §107(2)) turns on whether the original work is informational or creative. Unconsented copying or distribution is more likely to be considered fair if the original work was factual or informational, such as a news broadcast, instead of a creative work, such as a motion picture or a musical composition. *A&M Records, Inc. v Napster, Inc.* (9th Cir 2001) 239 F3d 1004, 1118; *Los Angeles News Serv. v Tullo* (9th Cir 1992) 973 F2d 791. Another aspect of this factor is whether the work is published or unpublished. The scope of fair use is broader with respect to published works. *Religious Technol. Ctr. v Netcom On-Line Communication Servs., Inc*. (ND Cal 1995) 923 F Supp 1231, 1245.

© The Regents of the University of California

§1.21 4. Portion of Work Used

The third factor (see 17 USC §107(3)) addresses both the amount of the original work copied and whether that amount constitutes the "heart" of the original work. In most cases, copying an entire work does not support a finding of fair use. *Religious Technol. Ctr. v Netcom On-Line Communication Servs., Inc*. (ND Cal 1995) 923 F Supp 1231, 1246, citing *Harper & Row, Publishers, Inc. v Nation Enters*. (1985) 471 US 539, 564, 85 L Ed 2d 588, 105 S Ct 2218. Moreover, "[c]opying even a small portion of a copyrighted work may exceed the boundaries of fair use if the material taken is the 'heart' of the work." *Los Angeles News Serv. v Tullo* (9th Cir 1992) 973 F2d 791, 798 (reproduction of most valuable part of certain news footage not protected by fair use doctrine). The amount of copying that is acceptable depends on the purpose and character of the use and the extent to which the copy transforms the original work. *Campbell v Acuff-Rose Music, Inc*. (1994) 510 US 569, 586, 127 L Ed 2d 500, 520, 114 S Ct 1164; *Religious Technol. Ctr. v Netcom On-Line Communication Servs., Inc*. (ND Cal 1995) 923 F Supp 1231, 1246.

© The Regents of the University of California

§1.22 5. Effect of Use on Market

The fourth factor considers the effect of the use on the potential market for, or value of, the copyrighted work. 17 USC §107(4). This factor has been identified as the most important element of fair use. "Fair use, when properly applied, is limited to copying by others which does not materially impair the marketability of the work which is copied." *Harper & Row, Publishers, Inc. v Nation Enters*. (1985) 471 US 539, 566, 85 L Ed 2d 588, 611, 105 S Ct 2218. A use is not fair if there is a meaningful likelihood of future harm to the copyright owner, and, if the use is commercial, the potential for harm may be presumed. *Los Angeles News Serv. v Tullo* (9th Cir 1992) 973 F2d 791, 798. Works that are transformative are considered less likely to adversely affect the market for the original work than works that merely supersede the original. *Kelly v Arriba Soft Corp.* (9th Cir 2003) 336 F3d 811.

© The Regents of the University of California

§1.23 L. First Sale

One of the exclusive rights of a copyright holder is the right to authorize or distribute copies of the work to the public. See §1.6. The "first sale" doctrine, embodied in 17 USC §109(a), is an important limitation on that right. It authorizes the owner of a lawfully made copy of a work to sell the copy without specific authorization from the holder of the copyright on the work, and thus terminates the right of the copyright holder to interfere with any subsequent resale or distribution of that particular copy. See generally *Parfums Givenchy v Drug Emporium* (9th Cir 1994) 38 F3d 477, 480, cert denied (1995) 514 US 1004; *Adobe Sys., Inc. v Stargate Software, Inc.* (ND Cal 2002) 216 F Supp 2d 1051. Historically, the "first sale" doctrine has had its principal application to retail sales and resales of books, records, and other tangible reproductions of copyrighted works. In 1990, §109 was amended specifically to exclude rentals, leases, licenses, and similar arrangements regarding sound recordings or computer software programs from the scope of the "first sale" doctrine. See 17 USC §109(b). In *Adobe Sys., Inc. v Stargate Software, Inc, supra,* the court held that the first sale doctrine did not apply to insulate a software reseller's sales of educational versions of software programs to buyers who were not students or educators, in violation of the terms of the reseller's distribution agreement with the software developer. Similarly, in *Pearson Educ. Inc. v Liao* (SD NY, May 13, 2008, 07-Civ-2423 (SHS)) 2008 US Dist Lexis 39222, the court found that the resale of "foreign edition" textbooks (textbooks manufactured and intended for sale abroad) within the United States on Internet sites was not protected under the first sale doctrine.

In *Video Pipeline v Buena Vista Home Entertainment, Inc.* (NJ 2002) 192 F Supp 2d 321, aff'd (3d Cir 2003) 342 F3d 191, cert denied (2004) 540 US 1178, an Internet website operator was enjoined from producing its own movie trailers from clips taken from plaintiff's films on video and distributing the trailers to the operator's on-line video retailer clients. The court held that the operator's actions were not protected by the "first sale" doctrine because the operator had not lawfully purchased copies of the plaintiff's films. Further, the court held that the operator did not stand in the shoes of its retailer clients and could not make use of defenses that might be available to them. The retailers had the right to advertise their copies of the copyrighted works, but even the retailers did not have the right to display images of the copyrighted works over the Internet.

NOTE: The distinction between a software license and the sale of that software is important both in the context of the first sale doctrine and in the context of the safe harbor for computer programs set forth in §117. See §1.16A. In *Vernor v Autodesk, Inc.* (WD Wash 2008) 555 F Supp 2d 1164, the court held that even though several copies of software had been transferred subject to a license that prohibited subsequent transfer of the copies, they were still subject to the §109 first sale doctrine and could therefore be resold in an eBay auction. The court relied on *U.S. v Wise* (9th Cir 1977) 550 F2d 1180, 1187, in which the Ninth Circuit analyzed various transfer contracts between film studios and the recipients of movie prints, and found that sales had taken place when the transferees were not required to return the print.

© The Regents of the University of California

II. DIGITAL MILLENNIUM COPYRIGHT ACT

§1.24 A. Introduction

The Digital Millennium Copyright Act (DMCA) (Pub L 105-304, 112 Stat 2860), codified in scattered sections of Title 17 of the United States Code, including 17 USC §§512, 1201-1205, and 1301-1332, amended existing copyright law to address emerging issues of the Internet age and to bring the United States more in line with international copyright policies and practices. The DMCA is divided into five sections: Title I, the WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998, implementing two 1996 World Intellectual Property Organization (WIPO) treaties; Title II, the Online Copyright Infringement Liability Limitation Act, which provides safe harbors against copyright infringement claims for online service providers; Title III, the Computer Maintenance Competition Assurance Act, which creates an exemption for making copies of computer programs for the purpose of maintenance and repair; Title IV, Miscellaneous Provisions, which includes new exceptions in the copyright act for libraries and for making ephemeral recordings and webcasting of sound recordings on the Internet; and Title V, the Vessel Hull Design Protection Act, which creates a new form of protection for hull design.

According to the legislative history, the DMCA was enacted to preserve copyright enforcement as well as to provide immunity to service providers from copyright infringement liability for passive, automatic actions of a service provider's system through a technological process initiated by another, without knowledge of the service provider. *ALS Scan, Inc. v RemarQ Communities, Inc.* (4th Cir 2001) 239 F3d 619, citing HR Conf Rep 105-796, 105th Cong, 2d Sess (1998), reprinted in 1998 US Code Cong & Ad News 639.

NOTE: Generally, courts have found DMCA violations only when there is an underlying Copyright Act violation. *Storage Technol. Corp. v Custom Hardware Eng'g & Consulting, Inc.* (Fed Cir 2005) 421 F3d 1307, 1313.

Sections 1.25-1.43 focus on two areas of interest for online businesses: anti-circumvention and limitation of liability for online service providers, addressed in Titles I and II, respectively, of the DMCA, which demonstrate both the enforcement and safeguard objectives of the Act.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/1 Copyrights and the DMCA/ B. Anti-Circumvention of Technological Protection Measures/§1.25 1. Anti-Circumvention Prohibitions (17 USC §1201)

B. Anti-Circumvention of Technological Protection Measures

§1.25 1. Anti-Circumvention Prohibitions (17 USC §1201)

Title I of the DMCA amends the Copyright Act by adding a new Chapter 12 on copyright protection and management systems (17 USC §§1201-1205). Title 17 USC §1201 includes prohibitions on both (a) conduct and (b) technology, products, services, devices, or components that circumvent technological measures designed to protect a copyrighted work. It addresses both measures to control access to copyrighted works and measures to prevent copying or infringement of any of the other exclusive rights associated with copyright ownership. Regarding *conduct,* §1201 provides that "[n]o person shall circumvent a technological measure that effectively controls access to a work protected under this title." 17 USC §1201(a)(1)(A). This prohibition applies only to controls on access, has no knowledge requirement, and applies regardless of whether any infringement results from the conduct. Circumvention of a technological measure means descrambling a scrambled work, decrypting an encrypted work, or otherwise bypassing, deactivating, or impairing a technological measure without authorization from the copyright owner. 17 USC §1201(a)(3)(A).

NOTE: Use of a valid user name and password to access a protected site does not violate the DMCA because it does not require descrambling, decrypting, avoiding, bypassing, removing, deactivating, or impairing a technological measure. *Egilman v Keller & Heckman, LLP* (D DC 2005) 401 F Supp 2d 105, 113.

In contrast, the subsection regarding *technology, products, services, devices, and components* prohibits circumvention of technological measures to control access as well as technological measures to control copying or infringement of other exclusive rights of copyright holders. Specifically, §1201(a)(2) prohibits anyone from manufacturing, importing, or otherwise providing any technology, product, service, device, or component that is (a) primarily designed or produced to circumvent a technological measure that effectively controls access to a copyrighted work, (b) has only limited commercial purpose other than circumvention, and (c) is knowingly marketed by or for that person for use in circumvention. 17 USC §1201(a)(2). See *Sony Computer Entertainment Am. Inc. v GameMasters, Inc.* (ND Cal 1999) 87 F Supp 2d 976, 981 (court enjoined defendant GameMasters from advertising, distributing, selling, or purchasing Game Enhancer, a device that circumvented CD encryption data preventing unauthorized games from being used on Sony PlayStation consoles). Section 1201(b) provides the same bar on any technology, product, service, device, or component that circumvents a technological measure that effectively protects the rights of a copyright owner in a copyrighted work. 17 USC §1201(b)(1)(A). See *RealNetworks, Inc. v Streambox, Inc.* (WD Wa, Jan. 18, 2000, No. C99-2070P) 2000 US Dist Lexis 1889 (defendants enjoined from manufacturing device that mimicked authentication sequence of plaintiff's receiver and fooled plaintiff's transmitter into streaming data to unauthorized receiver). See also *Universal City Studios, Inc. v Reimerdes* (SD NY 2000) 111 F Supp 2d 294, aff'd *sub nom Universal Studios, Inc. v Corley* (2d Cir 2001) 273 F3d 429 (defendants ordered to stop posting on their website copy of program that bypassed standard encryption protocol used by plaintiffs to prevent unauthorized copying of DVDs).

In *Lexmark Int'l, Inc., v Static Control Components, Inc.* (6th Cir 2004) 387 F3d 522, plaintiff Lexmark brought a claim under 17 USC §1201(a)(2), alleging that defendant had distributed "devices that circumvent access-control measures placed on copyrighted works." 387 F3d at 545. Specifically, defendant Static Control had created a computer chip that permitted after-market toner cartridges to operate with Lexmark's printers, notwithstanding a microchip designed by Lexmark to prevent Lexmark printers from functioning with toner cartridges that Lexmark had not refilled. 387 F3d at 546. In refusing to find liability under §1201(a)(2), the *Lexmark* court distinguished earlier cases such as *RealNetworks* and *Reimerdes,* in which access-control measures prevented or protected access to copyrightable material such as video games, CDs, or DVDs. In contrast, the measures implemented by Lexmark merely controlled access to functions of a Lexmark printer or toner cartridge. Moreover, to the extent that Lexmark had created a copyrightable access-control measure (in the form of a printer control program), Lexmark had not encrypted or otherwise protected that program, and the court could find no support for a claim under §1201(a) "where the access-control measure left the literal code or text of the computer program or data freely readable." 387 F3d at 547. Put differently, §1201(a) requires

controls on access to some copyrightable material (*e.g.*, music, movies, video games, software), and then has effect when a manufacturer (387 F3d at 548):

> prevents all access to the copyrightable material and the alleged infringer responds by marketing a device that circumvents the technological measure designed to guard access to the copyrightable material.

In *Lexmark,* these conditions were not met. Similarly, in *Chamberlain Group, Inc. v Skylink Technols., Inc.* (Fed Cir 2004) 381 F3d 1178, the court held that a universal transmitter that allowed users to access software embedded in "rolling code" garage door openers did not violate the DMCA because no nexus was shown to exist between the access provided and infringement of any copyrights.

Despite its prohibitions on production and sale of circumvention devices, the DMCA expressly states that it does not require manufacturers of consumer electronics or telecommunications or computing equipment to design their products in response to any particular technological measures. 17 USC §1201(c)(3). The sole exception to this rule is for analog videocassette recorders, which are now required to be designed to conform to certain specified technologies that prevent unauthorized copying of analog videocassettes and certain analog signals. 17 USC §1201(k). In addition, the DMCA expressly states that it is not intended to affect rights, remedies, limitations, or defenses to copyright infringement (including fair use) or to diminish or enlarge vicarious or contributory liability for copyright infringement or any rights of free speech or the press for activities using consumer electronics, telecommunications, or computing products. 17 USC §1201(c).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/1 Copyrights and the DMCA/§1.25A 2. Copyright Management Information (17 USC §1202)

§1.25A 2. Copyright Management Information (17 USC §1202)

The DMCA protects the integrity of copyright management information (CMI), which includes the title of the work, the name of the author, copyright owner or performer, the terms and conditions for use of the work, and "identifying numbers or symbols referring to such information or links to such information." 17 USC §1202(c). Removal or alteration of CMI is prohibited. 17 USC §1202(b).

The court in *IQ Group v Wiesner Publ'g, LLC* (D NJ 2006) 409 F Supp 2d 587, sought to narrow the statutory definition of CMI. The DMCA, the court found, "should not be construed to cover copyright management performed by people, which is covered by the Copyright Act… it should be construed to protect copyright management performed by the technological measures of automated systems." 409 F Supp 2d at 597. In granting summary judgment for the defendant, the court held that plaintiff's electronic logo, which contained a hyperlink that purportedly led to copyright information, did not constitute CMI because it was not part of "an automated copyright protection or management system functioning within a computer network environment." Therefore, the defendant's removal of the logo did not violate 17 USC §1202(b). 409 F Supp 2d at 598. Noting that Congress viewed digital watermarks as an example of CMI, the *IQ Group* court quoted a watermark provider's explanation of the process as enabling users "to embed into audio, images, video and printed documents a digital code that is imperceptible during normal use but readable by computers and software." 409 F Supp 2d at 596.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/1 Copyrights and the DMCA/§1.26 3. Exceptions to Anti-Circumvention Prohibitions

§1.26 3. Exceptions to Anti-Circumvention Prohibitions

The DMCA includes a number of exceptions to its anti-circumvention provisions. Most broadly, the DMCA creates an overall exemption for the lawful, authorized activities of law enforcement, intelligence gathering, and other government activities. 17 USC §1201(e). The remaining exceptions concern activities related to access to copyrighted works addressed in §1201(a). Section 1201(a)(1) creates an evolving exception for persons using certain classes of works who are or are likely to be adversely affected in their ability to make noninfringing uses of that particular class of works. The scope of this exception is to be determined in periodic rulemakings by the Librarian of Congress in consultation with other officials. 17 USC §1201(a)(1)(B)-(C). In its most recent rulemaking, effective November 27, 2006, the Librarian of Congress identified six classes of works exempt from the prohibition against circumvention of technological measures that control access to copyrighted works. The six classes are as follows (71 Fed Reg 68472 (2006)):

> 1. Audiovisual works included in the educational library of a college or university's film or media studies department, when circumvention is accomplished for the purpose of making compilations of portions of those works for educational use in the classroom by media studies or film professors.
>
> 2. Computer programs and video games distributed in formats that have become obsolete and that require the original media or hardware as a condition of access, when circumvention is accomplished for the purpose of preservation or archival reproduction of published digital works by a library or archive. A format shall be considered obsolete if the machine or system necessary to render perceptible a work stored in that format is no longer manufactured or is no longer reasonably available in the commercial marketplace.
>
> 3. Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. A dongle shall be considered obsolete if it is no longer manufactured or if a replacement or repair is no longer reasonably available in the commercial marketplace.
>
> 4. Literary works distributed in ebook format when all existing ebook editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling either of the book's read-aloud function or of screen readers that render the text into a specialized format.
>
> 5. Computer programs in the form of firmware that enable wireless telephone handsets to connect to a wireless telephone communication network, when circumvention is accomplished for the sole purpose of lawfully connecting to a wireless telephone communication network.
>
> 6. Sound recordings, and audiovisual works associated with those sound recordings, distributed in compact disc format and protected by technological protection measures that control access to lawfully purchased works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.

For a period of three years from the issuance of these rules, anyone making a noninfringing use of a work in any of the foregoing six classes of works is exempt from the anti-circumvention provisions of the DMCA. The Librarian is expected to announce the results of its latest rulemaking in late 2009. See Notice of Inquiry: Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (73 Fed Reg 58073 (2008)); Notice of Proposed Rulemaking: Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (73 Fed Reg 79425 (2008)). See also http://www.copyright.gov/1201.

The other exceptions to the anti-circumvention provisions of §1201(a) include the following:

- Access by nonprofit libraries, archives, and educational institutions to commercially exploited copyrighted works for the good faith purpose of determining the utility of such work for the institution. 17 USC §1201(d).
- Reverse engineering for the sole purpose of creating interoperability with other independently created programs. 17 USC §1201(f).
- Encryption research on lawfully obtained encrypted works after a good faith effort to obtain authorization. 17 USC §1201(g).
- Protection of minors, by allowing courts to consider the necessity of circumvention devices that prevent access of

materials on the Internet. 17 USC §1201(h).

- Protection against the collection and dissemination of personally identifying information and online activities. 17 USC §1201(i).
- Security testing, if the testing does not constitute an act of infringement under the Copyright Act or any applicable copyright law. 17 USC §1201(j).

Several exceptions to the DMCA's anti-circumvention provisions were reviewed and interpreted in *Universal City Studios, Inc. v Reimerdes* (SD NY 2000) 111 F Supp 2d 294, aff'd sub nom *Universal Studios, Inc. v Corley* (2d Cir 2001) 273 F3d 429. The plaintiffs were eight major U.S. motion picture studios; the defendants were hackers who posted on the Internet a program (DeCSS) that circumvented the plaintiffs' CSS (Content Scramble System) encryption system for DVDs. The defendants contended that their activities with regard to the program fell within the exception created in 17 USC §1201(f) for reverse engineering of a computer program to achieve interoperability with another independently created computer program. The court rejected this defense because the §1201(f)(3) exception allows only the person who acquired the information through reverse engineering to make it available to the others, and the defendant had not written the computer program but had acquired it from computer hackers who had created it. The court also rejected the defendant's claim that its activities were covered under the DMCA's exception for encryption research in 17 USC §1201(g). In granting injunctive and declaratory relief for the plaintiffs, the court considered whether the intended effect of dissemination was to advance encryption research or facilitate copyright infringement, whether the defendants obtained authorization from and communicated with the copyright owners, and whether a legitimate study of encryption existed. 111 F Supp 2d at 321.

PRACTICE TIP: Clients should be advised to consult with counsel and obtain consent from the copyright owner for any encryption research or reverse engineering of third party digital content.

The defendants' attempt to invoke the DMCA's security test exception (17 USC 1201(j)) also failed. The court found no indication that the DeCSS program had anything to do with testing computers, systems, or networks, and that the defendants had failed to seek authorization for their work. 111 F Supp at 321.

PRACTICE TIP: Clients should stay within the statutory limits of 17 USC §1201 when attempting to take advantage of an exception from the anti-circumvention provisions. Courts have applied the exceptions strictly.

© The Regents of the University of California

§1.27 4. Remedies

Remedies for persons injured by violations of 17 USC §1201 include civil suits in federal court for equitable relief or monetary damages similar to those already available under the Copyright Act. 17 USC §1203(c). In particular, a plaintiff may pursue actual damages suffered as a result of the violation, as well as any profits of the defendant attributable to the violation that are not included in the actual damages calculation. 17 USC §1203(c)(2). Alternatively, a plaintiff may elect (17 USC §1203(c)(3)(A))

> [a]t any time before final judgment is entered…to recover an award of statutory damages for each violation of section 1201 in the sum of not less than $200 or more than $2,500 per act of circumvention, device, product, component, offer, or performance of service, as the court considers *just*. [Emphasis added.]

Damages may be reduced for innocent violations. 17 USC §1203(c)(5)(A). Nonprofit libraries, archives, educational institutions, and public broadcasting entities are given special statutory protection against the imposition of damages if they can show that they were not aware and had no reason to believe that their actions constituted a violation. 17 USC §1203(c)(5)(B).

In *Sony Computer Entertainment Am., Inc. v Filipiak* (ND CA 2006) 406 F Supp 2d 1068—the first reported decision to construe the meaning of "just" for statutory damages under 17 USC §1201—the court looked to rulings involving statutory damages under the Copyright Act's remedies for infringement. See 17 USC §504(c). *Sony* involved the defendant's sale of devices that allowed users to play unauthorized and illegally copied video games on their Sony PlayStation and PlayStation 2 consoles. The court based its damages finding on case law factors such as the expense saved by the defendant in avoiding a licensing agreement, profits reaped by the defendant in connection with the infringement, revenues lost to the plaintiff, and the willfulness of the infringement. 406 F Supp 2d at 1074. The court defended its damages award as "necessary to discourage wrongful conduct by other potential retailers who might be tempted to engage in" lucrative but unlawful circumvention practices. 406 F Supp 2d at 1075.

© The Regents of the University of California

§1.28 5. Constitutional Issues: *U.S. v ElCom Ltd.*

Section 1201(b) of the Digital Millennium Copyright Act (17 USC §1201(b)) survived constitutional challenges on First and Fifth Amendment grounds in *U.S. v ElCom Ltd.* (ND Cal 2002) 203 F Supp 2d 1111. In that case, the government brought criminal charges against ElCom and its employee Dmitry Sklyarov for violation of 17 USC §1201(b)(1)(A) and (C), charging that the defendants developed and sold a product that allowed users to convert legitimately purchased eBooks into other formats that could easily be copied, printed, and transferred to others, effectively bypassing the eBook copyright holder's access and use controls.

In response to the defendants' claim that the DMCA was unconstitutional, the court first ruled that there was no statutory ambiguity concerning what tools were allowed and what tools were prohibited because the statute banned trafficking in all circumvention devices. Thus, the DMCA was not unconstitutionally vague for purposes of the due process clause of the Fifth Amendment. 203 F Supp 2d at 1125. Regarding alleged content-based restrictions on speech in violation of the First Amendment, the court held that while computer code was protected by the First Amendment to the extent that the DMCA impacts a lawful purchaser's right to make copies or space-shift copies from one computer to another, the limited impairment of that single right does not significantly compromise or impair the First Amendment rights of users so as to render the DMCA unconstitutionally overbroad. Finally, the court held that Congress had not exceeded its authority under the Commerce Clause by enacting the DMCA.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/1 Copyrights and the DMCA/§1.29 C. Limitations of Liability for Online Service Providers--Infringement Safe Harbors

§1.29 C. Limitations of Liability for Online Service Providers—Infringement Safe Harbors

Internet service providers (ISPs) and other vendors providing web hosting services for content posted by clients have been subject to claims for contributory or vicarious copyright infringement. See generally §§1.12-1.16. Such claims are particularly troublesome for ISPs because they usually lack actual knowledge of infringement, they may be unable to access or to adequately monitor content posted by their clients, and the cost of any such monitoring is usually prohibitive. Title II of the DMCA added a new §512 to the Copyright Act, providing four safe harbors limiting monetary liability and, in some cases, injunctive or other equitable relief that may be imposed on an ISP for copyright infringement by reason of the provider's storage or transmission of infringing material through its system or network. 17 USC §512. According to the legislative history, Title II was intended to protect ISPs from liability for direct, vicarious, and contributory infringement and to preserve "the strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment." *Hendrickson v eBay, Inc.* (CD Cal 2001) 165 F Supp 2d 1082, 1088 (quoting S Rep No. 105-190, 105th Cong, 2d Sess (1998), at 1). The safe harbors operate with respect to the following four functions, or categories of conduct, of ISPs (17 USC §512(a)-(d)):

- Transitory digital network communications, when the ISP is merely acting as a conduit by transmitting infringing material over the system or network at someone else's request;
- System caching, when the ISP is merely storing infringing material on a system or network temporarily and as an intermediate copy;
- Storage of information on systems or networks at the direction of users, when an ISP is merely storing infringing material at the request of another party; and
- Information location tools, when the ISP utilizes tools such as hyperlinks, directories, and search engines to refer users to sites that contain infringing material.

Qualifying for a safe harbor depends on compliance with general conditions that apply to all four safe harbors (see §1.30), as well as the specific conditions applicable to each safe harbor (see §§1.31-1.40). Each safe harbor is construed independently of the others; whether an ISP qualifies for one safe harbor is to be based solely on the criteria for that safe harbor, and does not affect the ISP's qualification under any other safe harbor. 17 USC §512(n). See generally *Perfect 10, Inc. v Cybernet Ventures, Inc.* (CD Cal 2002) 213 F Supp 2d 1146.

To counterbalance the limitations on liability for ISPs, §512 includes a subpoena power (see §1.41) enabling copyright owners to compel certain ISPs seeking safe harbor protection to disclose the names of their users who are allegedly infringing the copyrights of the complaining copyright holder. 17 USC §512(h). The subpoena power applies to service providers storing infringing material on their servers, but not to service providers acting as mere conduits. See *Recording Indus. Ass'n v Verizon Internet Servs., Inc.* (DC Cir 2003) 351 F3d 1229, cert denied (2004) 543 US 924; *Recording Indus. Ass'n v Charter Communications, Inc. (In re Charter Communications, Inc.)* (8th Cir 2005) 393 F3d 771. See also §1.41.

© The Regents of the University of California

§1.30 1. General Conditions for Safe Harbors

Certain conditions must be met in order for an ISP to take advantage of any of the four safe harbors. First, the party seeking to use the safe harbor must qualify as a "service provider" within the meaning of the DMCA. For the purposes of the first safe harbor regarding transmission of digital communications, a service provider is an entity offering transmission, routing, or connection of digital online communications of material selected by users between or among points specified by users, without modification of the content of the material. 17 USC §512(k)(1)(A). For the remaining safe harbors, a service provider is an entity that provides online services or network access, or an entity that operates facilities for online services or network access (including service providers described in §512(k)(1)(A)). 17 USC §512(k)(1)(B). The definition of "service provider" in §512(k)(1)(B) is very broad, and finding its limits in particular cases may be difficult. The definition was intended to include websites that provide location service tools, such as Yahoo!, as well as ISPs. See *Perfect 10, Inc. v Cybernet Ventures, Inc.* (CD Cal 2002) 213 F Supp 2d 1146, 1175 (alleged infringer was service provider, even though it did not host infringing images and infringing images did not pass through its computers).

Second, a service provider must (a) adopt, reasonably implement, and inform its subscribers of a policy for terminating in appropriate circumstances the accounts of subscribers who are repeat infringers, and (b) accommodate and not interfere with "standard technical measures" used by copyright owners to identify or protect copyrighted works. 17 USC §512(i). "Reasonable implementation" requires that the service provider have a working notification system and procedures for dealing with DMCA-compliant notifications. *Perfect 10, Inc. v CCBill LLC* (9th Cir 2007) 488 F3d 1102, 1109, cert denied (2007) ___ US ___, 169 L Ed 2d 553, 128 S Ct 709. The possibility of losing a safe harbor was intended to provide a strong incentive for service providers to cooperate with copyright holders and to ensure that judicial supervision played a secondary role to self-regulation. 213 F Supp 2d at 1178.

© The Regents of the University of California

§1.31 2. Transitory Digital Network Communications Safe Harbor (17 USC §512(a))

The transitory digital network communications safe harbor applies to a service provider acting as a data conduit by transmitting, routing, or providing connections for infringing material through a network or system controlled or operated by or for the service provider. 17 USC §512(a). This safe harbor includes the intermediate and transient storage of the infringing material in the course of transmission. A service provider may take advantage of the safe harbor if, in addition to the general conditions outlined in §1.30 above, the following conditions apply (§512(a)(1)-(5)):

- The transmission was initiated by or at the direction of a person other than the provider;
- The transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of material by the service provider;
- The provider does not select the recipients of the material (except as an automatic response to another person's request);
- Any copies made in the course of intermediate or transient storage are not accessible to anyone other than the anticipated recipients and are not accessible for a period longer than is reasonably necessary for the transmission, routing, or provision of connections; and
- The material is transmitted through the system without modification of its content.

The §512(a) exemption reflects the decision in *Religious Technol. Ctr. v Netcom On-Line Communication Servs., Inc.* (ND Cal 1995) 907 F Supp 1361, in which postings were stored on Netcom's servers and available to system users for up to eleven days. The court held that the provider was not liable for direct infringement because it took no affirmative action that directly infringed on the copyrighted works other than installing and maintaining a system in which software automatically forwarded messages received from subscribers and temporarily stored copies on its system. But see *Ellison v Robertson* (9th Cir 2004) 357 F3d 1072, 1081 (defendant service provider's failure to update contact information with Copyright Office prevented defendant from learning of certain infringing activities on Usenet newsgroups subject to 14-day storage period; lack of up-to-date contact information gave rise to issue of fact concerning whether defendant reasonably implemented policy of terminating repeat infringers under §512(i)).

Eligibility under the provisions of §512(a) also requires compliance with 17 USC §512(i), which requires an ISP to adopt, reasonably implement, and notify its members of a policy to terminate subscribers who are repeat infringers. Section 512(i) does not require the service provider to actually terminate repeat offenders or investigate infringement but to "put its users on notice that they face a realistic threat of having their Internet access terminated if they repeatedly violate intellectual property rights." *Ellison v Robertson* (CD Cal 2002) 189 F Supp 2d 1051, 1066, aff'd in part and rev'd in part on other grounds in *Ellison v Robertson* (9th Cir 2004) 357 F3d 1072; *Religious Technol. Ctr. v Netcom On-Line Communication Servs., Inc.* (ND Cal 1995) 907 F Supp 1361. See also *In re Napster, Inc. Copyright Litig*. (ND Cal 2002) 191 F Supp 2d 1087. But see *Ellison v Robertson* (9th Cir 2004) 357 F3d 1072, 1081.

A finding that a service provider is a secondary infringer does not rule out eligibility for the §512(a) safe harbor. In *A&M Records, Inc. v Napster, Inc.* (9th Cir 2001) 239 F3d 1004, 1025, the Ninth Circuit declined to uphold a district court ruling that alleged secondary infringers are never eligible for protection under §512(a).

© The Regents of the University of California

§1.32 3. System Caching Safe Harbor (17 USC §512(b))

A service provider may use the system caching safe harbor of 17 USC §512(b) if (a) the infringing material is made available online by a person other than the service provider; (b) the material is transmitted from such person, through the system or network, to another person at such other person's direction; and (c) storage is implemented by an automatic technical process for the purpose of making the material available to users who request access to it from the original infringer. 17 USC §512(b)(1). See *Parker v Google* (Ed Pa 2006) 422 F Supp 2d 492, 497, aff'd (3d Cir 2007) 242 Fed Appx 833, cert denied (2008) ___ US ___, 169 L Ed 2d 834, 128 S Ct 1101 (defendant entitled to safe harbor for automatic caching of web pages for indexing purposes); *Field v Google, Inc.* (D Nev 2006) 412 F Supp 2d 1106 ("cached" links to plaintiff's copyrighted works held to be fair use of those copyrighted works; defendant entitled to protection of system caching safe harbor). In addition to these conditions and the general conditions set forth in §1.30 above, the material must be transmitted without modification; the provider must comply with rules regarding refreshing, reloading, and other updating of material when specified by the person making the material available online and when in accordance with generally accepted data communications protocols; and the provider must not interfere with industry-standard tracking technology. 17 USC 512(b)(2).

The system caching safe harbor limits the liability of a service provider (who has met the other safe harbor requirements) only with regard to infringement that arises "by reason of" the caching of the material. *In re Aimster Copyright Litig.* (ND Ill 2002) 252 F Supp 2d 634, aff'd (7th Cir 2003) 334 F3d 643, cert denied (2004) 540 US 1107 (defendant's assertion that system caching safe harbor protected service providers "so long as" material in question was cached on system was overly broad reading of statute). The federal district court in *Aimster* also noted two other factors that ruled out the defendant's attempted use of the system caching safe harbor: The alleged infringing material was not transmitted "through" the defendant's system (17 USC §512(b)(1)(B)), nor was the material transmitted without modification (17 USC §512(b)(2)(A)).

© The Regents of the University of California

4. Safe Harbor for Information Residing on Systems or Networks at Direction of Users (17 USC §512(c))

§1.33 a. Generally

The safe harbor for information residing on systems or networks at the direction of users (17 USC §512(c)) may be used when a service provider hosts infringing material on websites or other repositories on its network at the direction of a user. In order for the provider to take advantage of this safe harbor, it must meet the following three-prong test (in addition to the general conditions stated in §1.30 above):

- The service provider (1) does not have actual knowledge that the material is infringing, or (2) in the absence of actual knowledge, is not aware of any facts or circumstances from which infringement is apparent, or (3) on obtaining such knowledge or awareness, acts expeditiously to remove or disable access to the infringing material (17 USC §512(c)(1)(A));
- When the service provider has the right and ability to control the infringing activity, the provider does not receive a financial benefit directly attributable to the activity (17 USC §512(c)(1)(B)); and
- Upon proper notification of the claimed infringement, in accordance with 17 USC §512(c)(3) (see §§1.37-1.39), the service provider acts expeditiously to remove or disable access to the infringing material (17 USC §512(c)(1)(C)).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/1 Copyrights and the DMCA/§1.34 b. Designation of Agent to Receive Notifications

§1.34 b. Designation of Agent to Receive Notifications

To take advantage of the §512(c) safe harbor, the service provider also must make available through its service (including on its website) the name, address, telephone number, e-mail address, and other contact information of an agent designated to receive notifications under 17 USC §512(c)(3) of copyright infringement. 17 USC §512(c)(2). This information must be on file with the Copyright Office and available for public inspection.

The Copyright Office currently does not provide an official form for designating an agent, but has issued regulations with a suggested format for interim designation of the agent (Interim Designation). See 37 CFR §201. The Interim Designation form, which is available on the Copyright Office's website at http://www.copyright.gov/onlinesp/index.html#agent, requests the following information:

- The full name and legal address of the service provider;
- All the names under which the service provider is doing business;
- The name of the designated agent;
- The full address, including a specific number and street name, of the agent (post office boxes are unacceptable unless they are the only address that can be used at that geographic location); and
- The agent's telephone number, fax number, and e-mail address.

The Interim Designation form must be signed by an officer or representative of the service provider. A filing fee is required. If the information regarding the agent changes, the company should file an amended Interim Designation. See http://www.copyright.gov/onlinesp/index.html#agent.

PRACTICE TIP: Counsel should monitor the Copyright Office website for future release of an official form for designation of agents to receive copyright infringement notifications under the DMCA. In addition, counsel should update changes in agent designation information promptly in order to avoid the potential liability faced by defendant AOL in *Ellison v Robertson* (9th Cir 2004) 357 F3d 1072 (see §1.31).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/1 Copyrights and the DMCA/§1.35 c. 'Right and Ability to Control'

§1.35 c. "Right and Ability to Control"

As noted in §1.33, the second prong of the 17 USC §512(c) safe harbor requires that if the service provider has "the right and ability to control" the infringing activity, it cannot receive a financial benefit from it. 17 USC §512(c)(1)(B). In *Hendrickson v eBay, Inc.* (CD Cal 2001) 165 F Supp 2d 1082, 1093, the court held that the concept of "right and ability to control" means more than a service provider's ability to remove or block access to materials posted on its system or stored in its database. Moreover, a service provider's limited monitoring of its website in a voluntary effort to combat Internet piracy does not indicate a "right and ability to control" infringing activity. 165 F Supp 2d at 1093. The *Hendrickson* court noted that the DMCA was not intended to discourage service providers from engaging in a monitoring program. 165 F Supp 2d at 1094. See also *UMG Recordings, Inc. v Veoh Networks, Inc.* (CD Cal 2009) 665 F Supp 2d 1099 (holding that safe harbor applies where users directed software functions that allowed them to access files via streaming and downloading); *Io Group, Inc. v Veoh Networks, Inc.* (ND Cal 2008) 586 F Supp 2d 1132 (determining that service provider qualified for safe harbor when it (1) could not control content its users uploaded, (2) responded and removed content on same day as DMCA-compliant notice was received, (3) did not encourage infringement, (4) had policed its system to maximum extent permitted by its architecture, and (5) was not required to prescreen submissions before publishing); *Perfect 10, Inc. v CCBill, LLC* (CD Cal 2004) 340 F Supp 2d 1077, 1104 (holding that safe harbor remains available to service provider whose "ability to control" is limited to disconnecting infringing clients).

© The Regents of the University of California

§1.36 d. Removal or Disabling Access to Infringing Material

The third prong of the 17 USC §512(c) safe harbor (see §1.33) requires the service provider, on proper notification of the claimed infringement, to act expeditiously to remove or block access to the infringing material. 17 USC §512(c)(1)(C). If the notice is not sufficient (see §1.37), the service provider's obligation to take down the infringing materials is not triggered. See *Perfect 10, Inc. v CCBill LLC* (9th Cir 2007) 488 F3d 1102, 1111, cert denied (2007) ___ US ___, 169 L Ed 2d 553, 128 S Ct 709 (notice of infringement that does not include "penalty of perjury" language does not "substantially" comply with §512(c)(3)(A)); *Hendrickson v eBay, Inc.* (CD Cal 2001) 165 F Supp 2d 1082, 1092.

Title 17 USC §512(g)(1) contains a general rule of nonliability for service providers that act in good faith to disable access to material claimed to be infringing or, based on the facts and circumstances, with respect to which infringement is apparent. If the service provider does act to take down alleged infringing materials, however, the provider must notify the subscriber responsible for the materials that the provider has done so, in order to qualify for this limitation of liability. 17 USC §512(g)(2)(A). If the subscriber sends the provider a counter-notification under 17 USC §512(g)(3), the service provider must take further action as discussed in §1.38 to remain eligible for the liability limitation.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/1 Copyrights and the DMCA/§1.37 e. Notification of Claimed Infringement; Safeguards Against Fraudulent Infringement Claims

§1.37 e. Notification of Claimed Infringement; Safeguards Against Fraudulent Infringement Claims

The safe harbor in 17 USC §512(c) includes requirements for notifying service providers of claimed infringement and safeguards against fraudulent infringement claims. A copyright owner claiming infringement must submit to the provider's designated agent a notice of alleged infringement which includes (17 USC §512(c)(3)(A)):

- A physical or electronic signature of the copyright owner (or someone authorized to act on behalf of the owner);
- Identification of the copyrighted work claimed to have been infringed;
- Identification of the infringing material to be removed, and information reasonably sufficient to permit the service provider to locate the material;
- Information reasonably sufficient to permit the service provider to contact the complaining party;
- A statement that the complaining party has a good faith belief that the use of the material is unauthorized by the copyright agent; and
- A statement that the information in the notification is accurate, and, under penalty of perjury, that the complaining party is authorized to act on behalf of the copyright owner.

Notice that substantially complies with the provisions of §512(c)(3) will not be deemed inadequate. 17 USC §512(c)(3); *ALS Scan, Inc. v RemarQ Communities, Inc.* (4th Cir 2001) 239 F3d 619, 626 (plaintiff's representative list of infringing photographs was easily identifiable by defendant service provider, and plaintiff's posting of copyright information was adequate notice of infringement).

In a recent decision, the Ninth Circuit Court of Appeals held that the defendant's notice of infringement, although mistaken, complied with the subjective "good faith belief" requirement of §512(c)(3) and precluded plaintiff's state tort law claims. *Rossi v Motion Picture Ass'n* (9th Cir 2004) 391 F3d 1000, 1004, cert denied (2005) 544 US 1018. But see *Hendrickson v eBay, Inc.* (CD Cal 2001) 165 F Supp 2d 1082, 1089 (notice inadequate for lack of attestations supporting its accuracy and the complaining party's right to act on behalf of the copyright owner, complainant's failure to state good faith belief that use of material was not authorized, and inadequate identification of infringing material). If a notification of claimed infringement is not adequate under §512(c)(3), the notice will not be considered in determining whether a service provider has actual or constructive knowledge of the infringing activity. 17 USC §512(c)(3)(B)(i); 165 F Supp 2d at 1092. See also *Hendrickson v Amazon.com, Inc.* (CD Cal 2003) 298 F Supp 2d 914.

PRACTICE TIP: Copyright owners requesting removal of copyrighted material under the DMCA should follow the notice requirements of 17 USC §512(c)(3)(A) strictly by providing adequate contact information, adequate descriptions of the copyright and the infringing material, and the required attestations, and should carefully document all actions taken.

Title 17 USC §512(f) provides civil damage penalties, including costs and attorney fees, against any person who knowingly and materially misrepresents certain information in a notification of infringement under 17 USC §512(c)(3) or a counter-notification under 17 USC §§512(g)(2)-(3) (see §1.38).

In *Online Policy Group v Diebold, Inc.* (ND Cal 2004) 337 F Supp 2d 1195, the court, in permitting plaintiffs to maintain an action for misrepresentation of copyright infringement, was required to interpret the language of §512(f) relating to a person who "knowingly materially misrepresents" that material or activity is infringing. 337 F Supp 2d at 1204. At issue in *Diebold* was an archive containing certain e-mail messages by employees of defendant Diebold, Inc. concerning, inter alia, the reliability of electronic voting machines produced by Diebold. On learning that the e-mail archive had become publicly available at a number of Internet sites, Diebold, citing the safe harbor provisions of the DMCA, sent cease and desist letters to a group of ISPs that included the *Diebold* plaintiffs. In granting summary judgment to plaintiffs on their §512(f) claim, the *Diebold* court held that Diebold "knew and specifically intended that" its cease and desist letters would prevent publication of the email messages concerning Diebold's voting systems, and that "[n]o reasonable copyright holder could have believed that the portions of the email archive discussing possible technical problems with Diebold's voting machines were protected by copyright." 337 F Supp at 1204.

In *Lenz v Universal Music Corp.* (ND Cal, Oct. 28, 2008, No. C07-3783JF(RS)) 2008 US Dist Lexis 91890, a YouTube.com user brought suit under §512(f) against Universal Music Corporation for a notification it sent to YouTube.com regarding a 29-second video the user posted of her baby dancing with a Prince song playing in the background. The court held that copyright owners must make "[a] good faith consideration of whether the particular use is fair use" as part of the initial review required by §512(c).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/1 Copyrights and the DMCA/§1.38 f. Counter-Notification by Subscriber; Restoration of Material

§1.38 f. Counter-Notification by Subscriber; Restoration of Material

Once a service provider notifies a subscriber that the service provider has removed or disabled access to the subscriber's allegedly infringing material, the subscriber may give the service provider a statutory counter-notification in an effort to have the material in question restored. See 17 USC §512(g)(2). Counter-notifications must be given in writing to the service provider's designated agent and must contain substantially the following elements (17 USC §512(g)(3)):

- A physical or electronic signature of the subscriber.
- A description of the material that has been taken down and the original location of the material before it was taken down.
- A statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled.
- The subscriber's name, address, and telephone number, and a statement that the subscriber consents to the jurisdiction of the federal district court for the judicial district in which the address is located (or if the subscriber is outside of the United States, that subscriber consents to jurisdiction of any judicial district in which the service provider may be found), and that the subscriber will accept service of process from the person who provided the original infringement notification.

To remain eligible for the statutory limitation of liability in 17 USC §512(g)(1) (see §1.36), on receipt of a counter-notification, the service provider must (1) promptly send the copyright owner a copy of the counter-notification, informing the copyright owner that the removed material will be restored in 10 business days (17 USC §512(g)(2)(B)), and (2) restore the removed material in not less than 10 and no more than 14 business days after receipt of the counter-notification, unless the copyright owner notifies the provider that it has filed an action seeking a court order to restrain the subscriber from engaging in the infringing activity (17 USC §512(g)(2)(C)). As discussed in §1.36, if the service provider takes these actions, it will be protected from any liability to the subscriber for having removed the material, regardless whether the material in question is ultimately determined to be infringing. 17 USC §512(g)(1)-(2).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/1 Copyrights and the DMCA/§1.39 g. Checklist: Notice and Take-Down Checklist

§1.39 g. Checklist: Notice and Take-Down Checklist

▶ To download **Word** version, right click and choose *Save Target As*

▶ To download **WordPerfect** version, right click and choose *Save Target As*

- Educate clients who are Internet Service Providers (ISPs) about DMCA safe harbors; advise ISP clients to notify counsel on receipt of an infringement notice and to consult with counsel as necessary to ensure compliance with safe harbor provisions.
- If a notice of infringement is received, review it for satisfaction of the statutory requirements (see §1.37).
- If the notice is deficient, immediately contact, or advise client to contact, the complaining party to collect the remaining information.
- Keep and/or advise the ISP to keep a record of infringement notices and any attempts made to contact the complaining party.
- If the notice substantially complies with the requirements, immediately advise the ISP to expeditiously continue with the take-down procedure.
- Immediately contact, or advise the ISP to contact, the ISP subscriber responsible for the allegedly infringing material to notify that subscriber of the alleged infringement and (1) to ensure the voluntary take-down of allegedly infringing materials by the subscriber or (2) to notify the subscriber of the involuntary take-down of allegedly infringing materials or the denial of access to the site.
- Verify, or advise the ISP to verify, the voluntary take-down of the infringing material, remove infringing materials, or deny access to the site on which the infringing materials reside.
- If the client receives a counter-notification from the ISP subscriber, review notice for satisfaction of statutory requirements (see §1.38).
- Immediately forward or advise the ISP to forward a copy of the counter-notification to the complaining party.
- Advise the ISP to replace the removed material within 10-14 days after receipt of a proper counter-notification if the ISP has not received notice that the complaining party has filed an action seeking a court order against the ISP client.
- Advise the ISP regarding possible obligations with respect to repeat copyright infringers.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/1 Copyrights and the DMCA/§1.40 5. Information Location Tools Safe Harbor (17 USC §512(d))

§1.40 5. Information Location Tools Safe Harbor (17 USC §512(d))

The information location tools safe harbor in 17 USC §512(d) provides that a service provider will not be liable for copyright infringement merely because it refers or links its users to an online location containing infringing material by way of hyperlinks, online directories, search engines, or other information location tools. 17 USC §512(d). The conditions under which this safe harbor will apply—including the absence-of-knowledge requirement, the financial benefit prohibition, and prompt removal of materials after notification of claimed infringement (see 17 USC §512(d)(1)-(3))—are nearly identical to the conditions applicable to the safe harbor for information residing on a service provider's network described in §§1.33-1.38. In addition, the provisions for notification of claimed infringement and counter-notifications (see §§1.37-1.38) of that safe harbor also apply to the information location tools safe harbor. 17 USC §512(d)(3), (g).

© The Regents of the University of California

§1.41 D. Subpoena Power (17 USC §512(h))

Under 17 USC §512(h)(1), a copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer. See generally *Recording Indus. Ass'n v Verizon Internet Servs., Inc.* (DC Cir 2003) 351 F3d 1229, cert denied (2004) 543 US 924. The request must include a copy of the notification of claimed infringement described in 17 USC §512(c)(3)(A) (see §1.37), a proposed subpoena, and a sworn declaration stating that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that the information will be used only for the purpose of protecting rights under the Copyright Act. 17 USC §512(h)(2). The clerk is authorized to issue the subpoena if the request and the subpoena conform to statutory requirements. 17 USC §512(h)(4). The subpoena will order the service provider to disclose expeditiously to the copyright owner information (to the extent available to the service provider) sufficient to identify the alleged infringer of the material described in the notification. 17 USC §512(h)(3). On receipt of the issued subpoena (either accompanying or after receipt of the infringement notification described in §512(c)(3)(A); see §1.37), the service provider must expeditiously disclose to the copyright owner (or person authorized by the copyright owner) the information required by the subpoena, notwithstanding any other provision of law and regardless of whether the service provider responds to the infringement notification. 17 USC §512(h)(5). The issuance and delivery of, and the remedies for noncompliance with, the subpoena are governed by the Federal Rules of Civil Procedure. 17 USC §512(h)(6).

The scope of the subpoena power under the DMCA is not unlimited. In *Recording Indus. Ass'n v Verizon Internet Servs., Inc.* (DC Cir 2003) 351 F3d 1229, cert denied (2004) 543 US 924, the District of Columbia Circuit held that 17 USC §512(h) does not authorize the issuance of a subpoena to an Internet service provider acting merely as a conduit for the transmission of information sent by others. Section 512(h) applies to an ISP that is storing infringing material on its servers, either as a temporary cache of a web page created by the ISP, or as a website stored on the ISP's server, or as an information locating tool hosted by the ISP. It does not apply to an ISP transmitting infringing material to or from a subscriber's personal computer. See also *Recording Indus. Ass'n v Charter Communications, Inc. (In re Charter Communications, Inc.)* (8th Cir 2005) 393 F3d 771.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/1 Copyrights and the DMCA/§1.42 E. Impact on Internet Service Providers

§1.42 E. Impact on Internet Service Providers

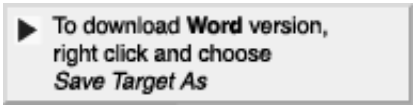
In enacting the DMCA, Congress sought not only to limit the liability of service providers, but also to help copyright owners protect their rights. To that end, service providers receive liability protection in exchange for assisting copyright owners to identify and deal with infringers, and copyright owners give up the right to sue service providers for vicarious infringement in exchange for that assistance. *In re Verizon Internet Servs., Inc.* (D DC 2003) 240 F Supp 2d 24, 36. See 17 USC §512(a)-(d), (h). To date, the courts are enforcing the DMCA safe harbors in accordance with their terms (see, *e.g., Ellison v Robertson* (9th Cir 2004) 357 F3d 1072; *Hendrickson v eBay, Inc.* (CD Cal 2001) 165 F Supp 2d 1082), and will deny immunity to ISPs with actual or constructive knowledge of infringing material (see *ALS Scan, Inc. v RemarQ Communities, Inc.* (4th Cir 2001) 239 F3d 619) or a direct financial interest in its distribution (see *Perfect 10, Inc. v Cybernet Ventures, Inc.* (CD Cal 2002) 213 F Supp 2d 1146; but see *Perfect 10, Inc. v Visa Int'l Serv. Ass'n* (ND Cal, Aug. 5, 2004, C04-0371JW) 2004 US Dist Lexis 15895 (distinguishing prior *Perfect 10* case based on defendant Visa's "content-neutral" services, whereas age verification services of Cybernet in prior case "materially contributed" to infringing actions)). ISPs should be aware of the requirements of each applicable safe harbor, and adjust their operations to the extent possible to comply with those requirements.

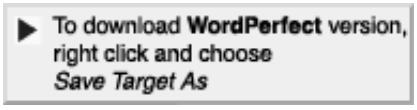
PRACTICE TIP: When evaluating possible courses of action for an e-business with respect to the DMCA, counsel should review the legislative history in addition to the statute, particularly if there is no case law on a particular issue. Courts have tended to give a great deal of weight to legislative history in interpreting the DMCA.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/1 Copyrights and the DMCA/§1.43 F. Checklist: Company DMCA Compliance Policy

§1.43 F. Checklist: Company DMCA Compliance Policy





Following is a checklist for DMCA compliance that may be useful to counsel representing Internet service providers:

- Ensure that the ISP has appropriate expertise and resources to deal with copyright issues.
- Consult with the ISP and determine which safe harbors may apply to it.
- Assist the ISP in developing or updating internal corporate policies and procedures on copyright consistent with the DMCA as well as traditional copyright law.
- Ensure that the ISP communicates the policy internally and trains employees to comply with it.
- Assist the ISP in developing a copyright compliance policy for client-users consistent with the DMCA.
- Ensure that the ISP notifies ISP subscribers of the copyright compliance policy.
- Ensure that the ISP warns its subscribers that their service will be terminated if they repeatedly violate the ISP's copyright policy or infringe the rights of copyright holders.
- Ensure that the ISP identifies a designated agent to receive notifications of alleged copyright infringement from the copyright owners.
- Assist the ISP in registering the designated agent with the Copyright Office (sample interim filing form at http://www.copyright.gov/onlinesp/index.html).
- Ensure that the ISP posts the designated agent's contact information in a conspicuous spot on its website.
- Counsel the ISP that it must accommodate and not interfere with technological measures that identify and protect copyrighted materials.
- Ensure that the ISP updates the designated agent contact information on its website and with the Copyright Office as necessary.
- Periodically visit the Copyright Office website for updates at http://www.copyright.gov.

© The Regents of the University of California

2

Patents and Trade Secrets

I. PATENTS
- A. Introduction §2.1
- B. What Is a Patent? §2.2
- C. What Is Patentable; Types of Patents §2.3
- D. Term of Patents §2.4
- E. Additional Requirements for Patentability
  - 1. Overview §2.5
  - 2. Origination §2.6
  - 3. Utility §2.7
  - 4. Novelty §2.8
  - 5. Nonobviousness §2.9
- F. Patent Applications
  - 1. Introduction §2.10
  - 2. Specification; Enablement; Best Mode §2.11
  - 3. Claims §2.12
  - 4. Statutory Time Bars §2.13
- G. International Issues §2.14
- H. Transferring Patents
  - 1. Introduction §2.15
  - 2. Form: Patent Assignment §2.16
  - 3. Form: U.S. Patent & Trademark Office Cover Sheet (Patents Only) §2.17
- I. Litigation Issues §2.17A
- J. Special Topics for Internet Businesses
  - 1. Business Method Patents §2.18
  - 2. Software Patents §2.19

II. TRADE SECRETS
- A. Introduction §2.20
- B. Definition of Trade Secret
  - 1. Statutory Definition §2.21
  - 2. Examples of Trade Secrets §2.22
  - 3. Computer Source and Object Code §2.22A
  - 4. Recipes, Manufacturing Processes §2.22B
  - 5. Customer Lists §2.23
- C. Loss of Trade Secret Protection §2.24
- D. Protection of Trade Secrets §2.25
  - 1. Departing Employees §2.26
  - 2. Practical Safeguards
    - a. Firewalls and Encryption §2.27
    - b. Physical Security §2.28
    - c. Managing Documents and Files §2.29
- E. Sample Company Policy on Trade Secret Protection
  - 1. Introduction §2.30
  - 2. Form: Company Policy on Trade Secret Protection §2.31
- F. Confidentiality Agreement
  - 1. Introduction §2.32
  - 2. Form: Confidentiality Agreement §2.33
- G. Misappropriation of Trade Secrets
  - 1. Asserting Claim of Misappropriation Under UTSA §2.34
  - 2. Defenses §2.35
  - 3. Damages §2.36
  - 4. Privilege and Disclosures Due to Litigation §2.37
  - 5. Economic Espionage Act of 1996 §2.38

© The Regents of the University of California

I. PATENTS

§2.1 A. Introduction

Companies doing business on the Internet that develop new business models or technology have an interest in protecting those inventions. If the invention involves software, the written code may be protected under copyright, but because copyright only protects the tangible expression of ideas and not ideas themselves (see §1.2), companies will need to look to other forms of intellectual property protection. Two methods of protecting the ideas behind inventions are discussed in this chapter: patents and trade secrets.

Patents are an important form of intellectual property protection because the owner of a patent can prevent others from using the patented invention for the term of the patent. Moreover, a patent owner can obtain revenue from its patent by licensing the invention and charging a fee for others to use it. For these reasons, the ownership of patented technology tends to reflect favorably on the financial valuation of an Internet-based business.

Generally speaking, "Internet patents" protect some aspect of the functionality or operation of an Internet website or a particular way of doing business online. One class of Internet patents that has received notoriety is generally referred to as "business method patents." As discussed in §2.18, in 1988 the Court of Appeals for the Federal Circuit departed from previously understood principles and ruled that a business method can be patented if it produces a useful, concrete, and tangible result. See *State St. Bank & Trust Co. v Signature Fin. Group* (1998) 149 F3d 1368, 1375, cert denied (1999) 525 US 1093. Before this decision, the patentability of mere "business methods" was uncertain. Since 1998, an increasing number of patents have been issued to software and Internet-based companies that have devised novel ways of doing business, which usually combine software with business methodology.

Sections 2.2-2.19 briefly discuss what a patent is, what is patentable, the requirements for patentability, the major elements of a patent application, and two special topics of particular importance for e-businesses: business method patents and software patents. Because patent law is such a specialized area of law, general corporate counsel for an e-business should consult experienced patent counsel for specific advice concerning the patentability of particular inventions and patent strategies. The following overview of patent law basics is not comprehensive. For a more extensive discussion of patent law, see California Business Litigation, chap 8 (Cal CEB 2002). See generally Chisum, Donald S. Patents: A Treatise on the Law of Patentability, Validity and Infringement (2003).

© The Regents of the University of California

§2.2 B. What Is a Patent?

Patent rights are created by, and subsist under, federal law exclusively. Under the U.S. Constitution, Congress has the power "[t]o promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries." US Const art I, §8, cl 8. A patent is a federal grant, under the Patent Act of 1952 as amended (35 USC §§100-376), of exclusive rights to an inventor for a limited period of time covering the right to use, manufacture, license, and sell an invention. A patent owner has the right to "exclude others from making, using, offering for sale, or selling [the patented] invention throughout the United States or importing the invention into the United States." 35 USC §154(a). The holder of a patent on a process also has the right to exclude others from making, using, offering for sale, or selling throughout the United States, or importing into the United States, products made by that process. 35 USC §154(a). A patent owner has the further right to prohibit others from inducing infringement or contributing to the infringement of a patent. 35 USC §271(b). Patents and patent applications are administered by the United States Patent and Trademark Office (USPTO). See http://www.uspto.gov.

The fundamental purpose of the patent system is to encourage early disclosure of inventions into the marketplace (*W.L. Gore & Assocs., Inc. v. Garlock, Inc*. (Fed Cir 1983) 721 F2d 1540, 1550, cert denied (1984) 469 US 851):

> As between a prior inventor who benefits from a process by selling its product but suppresses, conceals, or otherwise keeps the process from the public, and a later inventor who promptly files a patent application from which the public will gain a disclosure of the process, the law favors the latter.

A patent is not a guarantee that infringement will not occur, and the U.S. government has no role in preventing infringement of patents held by private parties. Defending a patent against claims of invalidity and obtaining judgments against infringing parties can cost an Internet-based business a considerable amount of money. However, the costs of litigating patent infringement suits may be offset by the availability of treble damages from infringers. See 35 USC §284.

NOTE: In *Microsoft Corp. v AT&T Corp.* (2007) 550 US 437, 167 L Ed 2d 737, 127 S Ct 1746, the Supreme Court held that copies of patented computer software—that was sent from the United States to a foreign computer manufacturer and then copied by the foreign manufacturer and installed on computers made and sold abroad—were not supplied from the United States and therefore were not protected by the Patent Act. Noting that the Digital Millennium Copyright Act had updated of copyright law, the Court suggested that Congress consider whether patent law should be augmented "to account for the realities of software distribution." 167 L Ed 2d at 753.

© The Regents of the University of California

§2.3 C. What Is Patentable; Types of Patents

The Patent Act states that anyone who "invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent" for that invention or discovery. 35 USC §101. The range of patentable subject matter under the Patent Act is broad, and new forms of technology initially deemed unpatentable by the USPTO may later be held patentable by the courts. In one famous court case, the Supreme Court held that in drafting the Patent Act, Congress intended to extend the realm of patentable subject matter to "anything under the sun that is made by man." *Diamond v Chakrabarty* (1980) 447 US 303, 309, 65 L Ed 2d 144, 150, 100 S Ct 2204, quoting HR 1923, 82d Cong, 2d Sess (1952).

While this is an extremely broad standard, the Supreme Court has also recognized that certain categories of subject matter remain unpatentable: "laws of nature, natural phenomenon, and abstract ideas." *Diamond v Diehr* (1981) 450 US 175, 180, 67 L Ed 2d 155, 164, 101 S Ct 1048. One common illustration of an unpatentable "abstract idea" is a mathematical formula, under the so-called "mathematical algorithm exception." *Diamond v Diehr, supra*; *AT&T Corp. v Excel Communications, Inc.* (Fed Cir 1999) 172 F3d 1352, cert denied (1999) 528 US 946. But see *In re Alappat* (Fed Cir 1994) 33 F3d 1526, 1544 (when mathematical algorithm is part of larger structure or process, it is patentable); §2.19. Printed matter is another exception to patentability. See *In re Lowry* (Fed Cir 1994) 32 F3d 1579; *In re Miller* (CCPA 1969) 418 F2d 1392.

The Patent Act establishes three types of patents, covering three distinct types of subject matter: utility patents, design patents, and plant patents. Utility patents are the most common and may be obtained for any new and useful process, machine, manufacture, or composition of matter, or any new or useful improvement thereof. Although the phrase "utility patent" is not in the Patent Act, the term is used to describe patents for inventions within the scope of 35 USC §101. Design patents protect new, original, and ornamental designs for manufactured articles. 35 USC §171. Design patents protect only the ornamental appearance of manufactured products, in contrast to utility patents, which protect the structure and function of useful inventions. Plant patents protect distinct new varieties of plants, including cultivated sports, hybrids, and mutations. 35 USC §161. Because Internet-based businesses are likely to be concerned only with utility patents, the following sections focus on utility patents.

PRACTICE TIP: The USPTO establishes guidelines for use by its examiners in evaluating patent applications. These guidelines evolve over time. The current USPTO Manual for Patent Examining Procedure (MPEP), 8th Edition, August 2001 (rev August 2006) is available at the USPTO website, http://www.uspto.gov/web/offices/pac/mpep/mpep.htm. In addition to the MPEP, the USPTO often publishes papers (also available at the USPTO website) on its current position regarding patents in certain subject areas. See, *e.g.,* the USPTO's papers on business method patents, at http://www.uspto.gov/web/menu/pbmethod.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/2 Patents and Trade Secrets/§2.4 D. Term of Patents

§2.4 D. Term of Patents

Utility and plant patents filed after June 8, 1995, have a term that begins at the initial filing date of the patent application and continues for a period of 20 years thereafter. 35 USC §154(a)(2). All utility patents that were pending as applications or were previously issued and enforceable on June 8, 1995, will expire at the later of either 17 years after the issue date or 20 years after initial filing date of the application. The term of design patents is 14 years from the date of grant. 35 USC §173. The term of a patent can be extended through a special act of Congress, but such extensions are rarely granted. After the term of a patent has elapsed, the patented invention falls into the public domain and may be used by anyone.

PRACTICE TIP: While patents offer strong intellectual property protection, a patent may not be the longest lasting form of intellectual property protection under United States law. If a particular invention is not easily reverse-engineered or reproduced, it may be in the interest of an e-business to maintain trade secret protection over the invention rather than obtaining a patent. See generally §§2.20-2.23. The term of protection for a trade secret is generally the period in which the owner can maintain it as secret. A classic example of a patentable invention that has never been patented but remains protected as a trade secret is the formula for Coca-Cola.

Patent terms should be taken into consideration when drafting patent licenses so that a licensee is not obligated to make royalty or other payments for use of a patented invention after the term of the patent has expired. Licenses usually contain language terminating payment obligations when the patent expires or if the patent is later declared invalid.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/2 Patents and Trade Secrets/ E. Additional Requirements for Patentability/§2.5 1. Overview

E. Additional Requirements for Patentability

§2.5 1. Overview

In addition to the subject-matter requirements discussed in §2.3, an invention must meet the requirements of origination, utility, novelty, and nonobviousness to qualify for a patent. See §§2.6-2.9. Further, the patent application itself must meet certain disclosure requirements. See §§2.10-2.12. Each of these requirements has been the subject of extensive interpretation, and any determination of patentability or infringement should be made by qualified patent counsel.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/2 Patents and Trade Secrets/§2.6 2. Origination

§2.6 2. Origination

A patent will not be issued to a person who did not invent the subject matter sought to be patented. 35 USC §102(f). Thus, the person filing a patent application must be the inventor of the subject matter of the application. Joint applications are permitted for inventions made by two or more co-inventors. See 35 USC §§116, 262.

© The Regents of the University of California

§2.7 3. Utility

Title 35 USC §101 limits the availability of patents to "useful" inventions. The Supreme Court has stated that a patent should not be issued for an invention that "has no known use or is useful only in the sense that it may be an object of scientific research." *Brenner v Manson* (1966) 383 US 519, 535, 16 L Ed 2d 69, 77, 86 S Ct 1033. To meet this requirement, a claimed invention must have a use or purpose and must actually accomplish that use or purpose. In short, the invention must claim to do something useful and then must actually do what it claims to do. An inventor cannot claim a patent on the impossible. A frequently cited example of a claimed invention that fails the utility test because it is deemed impossible to create is a perpetual motion machine. See *Newman v Quigg* (Fed Cir 1989) 877 F2d 1575, 1582 (energy-producing device violating laws of thermodynamics deemed unpatentable for "lack of utility" and "lack of enablement"). Whether a claimed invention has a useful purpose is a very low threshold; in general, an invention that has any use will be deemed patentable.

© The Regents of the University of California

§2.8 4. Novelty

Under 35 USC §101, a process or product must be "new" or "novel" to qualify for a patent. The novelty of an invention is determined by comparing what is claimed in the patent application to prior publications, patents, disclosures, or activities that are relevant to the invention. For example, under 35 USC §102(a), an invention will not qualify as "new" or "novel" if it was known or used by others in the United States, or patented or described in a printed publication in the United States or a foreign country before the date that the claimed invention was created. Section 102(b), (d), (e), and (g) describe other actions and disclosures in relation to the date of the patent application that must be considered in determining novelty. See also §2.13. The prior publications, patents, and other disclosures referred to in §102(a), (b), (d), (e) and (g) are generally known as "prior art."

Novelty is a question of fact, which involves an examination of the prior art in relation to the claimed invention. See USPTO, Manual for Patent Examining Procedure, (MPEP), 8th Edition, August 2001 (rev August 2006) chap 900, available at the USPTO website, http://www.uspto.gov/web/offices/pac/mpep/mpep.htm, for the protocol used by the USPTO in researching prior art. If every element of an invention is found to correspond to prior art, the invention is said to be "anticipated" by the existing prior art and is therefore not patentable. This is a low standard because a claimed invention need only have one element different from a prior invention to be meet the novelty standard. See generally *Glaverbel Societe Anonyme v Northlake Mktg. & Supply, Inc.* (Fed Cir 1995) 45 F3d 1550, 1554.

© The Regents of the University of California

§2.9 5. Nonobviousness

A patent may not be obtained (35 USC §103(a)):

> if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains.

In *Graham v John Deere Co*. (1966) 383 US 1, 17, 15 L Ed 2d 545, 556, 86 S Ct 684, the U.S. Supreme Court established a three-part analysis to determine obviousness or nonobviousness. First, the scope and content of the prior art must be identified. See 35 USC §102; §2.8. Once the prior art is identified, the differences between the prior art and the claimed invention must be ascertained. Third, the level of skill for someone with "ordinary skill in the art" must be established. This involves the hypothetical creation of a person with ordinary skill in the art rather than an analysis of the skill that an actual person possesses. For example, if the patent involved the field of physics, a person with ordinary skill in the art would be the ordinary skill of an average physicist, and not the skill possessed by Albert Einstein. See also *Environmental Designs, Ltd. v Union Oil Co.* (Fed Cir 1983) 713 F2d 693, 696, cert denied (1984) 464 US 1043.

In *Graham,* 383 US at 17, 15 L Ed 2d at 556, the Supreme Court stated that the analysis of nonobviousness "is one of inquiry and not quality." Secondary considerations, including "commercial success, long felt but unsolved needs, failure of others, etc." may also be used to evaluate whether the invention is obvious. For example, the more difficult an invention is to create and the more people who previously attempted but failed to create the invention or solve the problem, the greater the chance of a patent being granted for what otherwise might represent only a small improvement over the prior art. Moreover, when assessing obviousness, courts are to use an "expansive and flexible approach" and bar patentability because of obviousness if the invention is within the grasp of a person of ordinary skill in the relevant art, and the benefit of the innovation would be obvious. *KSR Int'l Co. v Teleflex Inc.* (2007) 550 US 398, 421, 167 L Ed 2d 705, 724, 127 S Ct 1727.

© The Regents of the University of California

F. Patent Applications

§2.10 1. Introduction

The process by which a patent is obtained from the USPTO is generally referred to as patent prosecution. To initiate the process, a written application must be filed with the USPTO. 35 USC §111(a)(1). The application must include a specification (see §§2.11-2.12), a drawing as necessary for an understanding of the subject matter of the invention, and an oath of the applicant that he or she is the original and first inventor of the invention. See 35 USC §§111(a)(2), 113, 115. Practitioners should consult the patent application guides published by the USPTO for further information. See, *e.g.,* United States Patent & Trademark Office, A Guide to Filing A Non-Provisional (Utility) Patent Application, available at http://www.uspto.gov/web/offices/pac/utility/utility.htm. Applications for certain patents can be filed electronically; guidelines for electronic filing are available on the USPTO website at http://www.uspto.gov/ebc/efs_help.html.

Following receipt of an application, the USPTO assigns the application to a patent examiner who is familiar with the subject area of the patent. See 35 USC §131; 37 CFR §1.104. With reference to the Patent Act, the USPTO's rules set forth in 37 CFR §§1.1-1.997, and the USPTO's patent examining manuals, the examiner will evaluate the claimed invention and, after almost certain negotiations between the inventor (or the inventor's counsel) and the examiner regarding the merit and scope of the claimed invention, either issue the patent or reject the application. If a patent application is rejected by the USPTO examiner, the inventor may appeal to the USPTO's Board of Patent Appeals and Interferences (see 35 USC §134) and, if necessary from there, to the U.S. Court of Appeals for the Federal Circuit (see 35 USC §141).

PRACTICE TIP: Although it is not required under United States law, marking a patented product offers the patent holder significant advantages. If the goods are not marked, damages may not be recovered in an infringement action except on proof that the infringer was notified of the infringement and continued to infringe thereafter. Damages may be recovered only for infringement occurring after such notice. Marking provides the infringer with constructive notice of the patent holder's claims. The marking must contain the word "patent" (or the abbreviation "pat.") and the patent number. If the goods themselves cannot be marked or labeled, the marking may go on the packaging. 35 USC §287(a). In the case of a website, a recent opinion has confirmed that marking the site constitutes constructive notice for purposes of §287(a). *Soverain Software, LLC v Amazon.com, Inc.* (ED Tex 2005) 383 F Supp 2d 904 (court rejected plaintiff's argument that marking is not required because Internet site is intangible object); *IMX, Inc. v Lending Tree, LLC* (D Del 2005) 79 USPQ2d 1373 (when patented software accessed through website, court found website to be "intrinsic" to patented system and held failure to mark website resulted in failure of required notice).

© The Regents of the University of California

§2.11 2. Specification; Enablement; Best Mode

Patent applications require significant and meaningful disclosure regarding almost every aspect of the claimed invention. The Supreme Court has stated that a patent "must describe the exact scope of an invention and its manufacture to 'secure to [the patentee] all to which he is entitled, [and] to apprise the public of what is still open to them.'" *Markman v Westview Instruments, Inc.* (1996) 517 US 370, 373, 134 L Ed 2d 577, 581, 116 S Ct 1384, quoting *McClain v Ortmayer* (1891) 141 US 419, 424, 35 L Ed 800, 802, 12 S Ct 76. The heart of a patent application is the specification, which must include a written description of the claimed invention setting forth the "manner and process of making and using [the claimed invention], in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and … the best mode contemplated by the inventor for carrying out his invention." 35 USC §112. To comply with the written description requirement, the applicant must convey with reasonable clarity to persons skilled in the art that the applicant invented the claimed invention. *Vas-Cath, Inc. v Mahurkar* (Fed Cir 1991) 935 F2d 1555, 1563.

The written description requirement is distinct from the so-called enablement requirement. *Vas-Cath, Inc. v Mahurkar, supra*. Under 35 USC §112, the description must be sufficient to enable someone with ordinary skill in the art to recreate and use the invention. See *In re Wands* (Fed Cir 1988) 858 F2d 731, 737; *W.L. Gore & Assocs., Inc. v. Garlock, Inc*. (Fed Cir 1983) 721 F2d 1540, 1556, cert denied (1984) 469 US 851. Without the enablement requirement, issuance of a patent would not be meaningful because even after expiration of the patent, the public would not be able to take advantage of the patented invention.

Another element of 35 USC §112 is the best mode requirement, which obligates the applicant to disclose what he or she believes is the best form or version of the claimed invention. This requirement is intended to prevent applicants from disclosing only an inferior or inefficient version of their of their invention to obtain the benefit of a patent monopoly, while keeping the best way to practice the claimed invention secret, thereby deriving an additional commercial advantage. *Amgen v Chugai Pharm. Co*. (Fed Cir 1991) 927 F2d 1200, 1209. The best mode for software-related inventions can be disclosed by describing the function of the software without including flow charts or divulging the source code, because writing the code is viewed as normally within the skill of a person in the art, not requiring undue experimentation. *Fonar Corp. v General Elec. Co*. (Fed Cir 1997) 107 F3d 1543, 1549, cert denied (1997) 522 US 908.

Both the enablement and best mode requirements reflect the general purpose of the patent system to provide early disclosure of inventions as justification for the granting of a patent. See §2.2. While the utility, novelty, and nonobviousness requirements are directed toward the invention itself, the enablement and best mode requirements are disclosure obligations of the inventor, designed to ensure that enough information about the claimed invention is released to the public to warrant issuance of a patent.

© The Regents of the University of California

§2.12 3. Claims

Title 35 USC §112 requires the specification to "conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention." The claims define the legal boundary of the inventor's patent rights. A claim is a single sentence, often containing several parts or steps, known as elements, describing the invention and its function. Each claim constitutes a separately defined invention, which is analyzed independently from any other claims in the patent application. An issued patent protects only what is claimed in the patent application, which may differ from the actual product or process created by the inventor. As a result, claims are almost always the subject of negotiation with the USPTO examiner and the inventor.

In a patent infringement case, the focus is normally on the construction and interpretation of claims. This involves a two-step process. First, the meaning and scope of the claims of the patent alleged to be infringed are analyzed for validity. This is a question of law, to be determined solely by the judge. Then, the infringing invention is compared with the patent's valid claims, and the jury is asked to consider whether infringement has occurred. See *Markman v Westview Instruments, Inc.* (Fed Cir 1995) 52 F3d 967, 976, aff'd (1996) 517 US 370. Claims are read narrowly; a claim "secures a process, a machine, a manufacture, a composition of matter, a design, but never the function or result of either, nor the scientific explanation of their operation." 517 US 370 at 373, 134 L Ed 2d at 582.

© The Regents of the University of California

§2.13 4. Statutory Time Bars

Even if a claimed invention meets the utility, novelty, and nonobviousness requirements and the application meets the disclosure requirements, a patent will not be issued if certain actions were taken or disclosures were made regarding the claimed invention more than one year before the date that the patent application was filed. See 35 USC §102. The patent system is designed to encourage *early* disclosure of patents; therefore, Congress placed certain limits on disclosure or use of a claimed invention before a patent application is filed as a condition of patentability. These limitations are directly related to the novelty requirement, discussed in §2.8.

If, more than one year prior to patent application filing date in the United States, a claimed invention was in "public use" or was "on sale" in the United States or was patented or described in a printed publication in the United States or abroad, a patent may not be issued. 35 USC §102(b). The rationale for withholding a patent in those circumstance includes:

> (1) discouraging removal of inventions from the public domain that the public reasonably has come to believe are freely available; (2) encouraging the prompt and widespread disclosure of inventions; (3) allowing an inventor a reasonable amount of time following sales activity to determine the potential economic value of a patent; and (4) prohibiting an inventor from commercially exploiting his invention beyond the statutorily prescribed time.

Quinton Instruments Co. v Impra, Inc. (In re Mahurkar Double Lumen Hemodialysis Cathetar Patent Litig.) (Fed Cir 1995) 71 F3d 1573, 1577, citing *Envirotech Corp. v Westech Eng'g, Inc.* (Fed Cir 1990) 904 F2d 1571, 1574.

Inventors should be extremely cautious about pre-application activities that may trigger the statutory bars to issuance of a patent and should consult with patent counsel to discuss potential pre-application uses of a patentable invention. Offers for sale, product announcements, product demonstrations at trade shows, disclosure of the invention in articles or magazines, and similar activities that take place before the statutory period may result in rejection of a patent application. In evaluating whether a patent application should be rejected or a patent invalidated because of the "on sale" bar, a court will examine the totality of circumstances surrounding the patent in view of the rationale for the "on sale" bar. *Quinton Instruments Co. v Impra, Inc. (In re Mahurkar Double Lumen Hemodialysis Cathetar Patent Litig.)* (Fed Cir 1995) 71 F3d 1573, 1576.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/2 Patents and Trade Secrets/§2.14 G. International Issues

§2.14 G. International Issues

The major difference between United States patent law and international patent law is the "first-to-invent" versus "first-to-file" distinction. The United States uses a "first-to-invent" system that attempts to award patents to the original creator of a particular invention. In the United States, the party first to invent is the party who is first to conceive of the particular invention. Even if at conception the invention does not yet function, the party first to conceive will still be given the benefit of the conception date provided that such party diligently continues to work to reduce the invention to practice. See *Agawam Co. v Jordan* (1869) 74 US 583, 19 L Ed 177; *Rex Chainbelt Inc.v Borg-Warner Corp*. (7th Cir 1973) 477 F2d 481, 487.

NOTE: The website of the World Intellectual Property Organization (WIPO), http://www.wipo.int, is an important source of information concerning international protection of patents and other intellectual property.

The internationally more common "first-to-file" system awards patents to the inventor that is first to file an application for a particular invention. The United States is party to international treaties, including the Paris Convention for the Protection of Industrial Property of March 20, 1883, as amended (available at http://www.wipo.int/treaties/en/ip/paris/pdf/trtdocs_wo020.pdf) and the Patent Cooperation Treaty of June 19, 1970, as amended (available at http://www.wipo.int/pct/en/texts/articles/atoc.htm), each of which attempts to harmonize the differences among the laws of signatory countries. In general, the Paris Convention allows patent applications filed in any member country also to be filed in any other member country within one year of the first filing date and to be backdated to the date of the initial application. This allows foreign patent applicants a one-year grace period to file in the United States and still establish a date of invention in the United States based on the initial foreign application filing date. It also allows United States inventors to file in foreign countries and receive the priority filing date that matches the date of such inventor's United States patent application.

PRACTICE TIP: Because the United States uses a "first-to-invent" system, inventors (and their employers) should keep copious notes regarding the invention and development of patentable items. Evidence such as lab notebooks can be valuable in establishing an invention date with the USPTO or the courts.

The Patent Cooperation Treaty (PCT) attempts to standardize the format and information disclosures required for a patent application in each of the member countries. The PCT recognizes that filing multiple applications around the world can be burdensome and expensive, and that the cost can be reduced if the basic information required by member countries is the same.

PRACTICE TIP: Despite these treaties, international patents are subject to each applicable nation's laws regarding patentable subject matter, fees required, the scope of patentability, and the term of patents. Counsel faced with international patent issues must consult with experienced patent counsel in each relevant jurisdiction to create and implement a patent strategy that will maximize the scope of patent protection for an invention.

The filing of an international application via the PCT constitutes an election of all types of protection available in all possible jurisdictions under the treaty. The decision as to the specific type of protection required in each country may be deferred until the date on which the applications are submitted in the local jurisdictions where foreign protection is sought, which may take place up to 30 months from the priority date of the application.

© The Regents of the University of California

H. Transferring Patents

§2.15 1. Introduction

The Patent Act provides that patents, patent applications, and any interest in a patent or a patent application are assignable in law by a written instrument. 35 USC §261. Similarly, a patent applicant, patentee, or his or her assigns or legal representatives may grant an exclusive license to the whole or any part of a patent or patent application. 35 USC §261.

NOTE: The transfer rules in 17 USC §261 do not apply to nonexclusive licenses of patents. Theoretically at least, nonexclusive patent licenses may be granted orally or even implied from conduct. A nonexclusive patent license has been described as a "mere waiver" of the right to sue the licensee for infringement. *Everex Sys. v Cadtrak Corp. (In re CFLC, Inc.)* (9th Cir 1996) 89 F3d 673, 677. For a discussion of exclusive and nonexclusive patent licenses, see California Business Litigation §§8.103-8.114 (Cal CEB 2002).

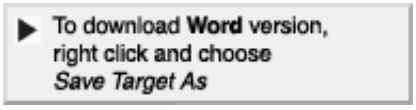
Notarial acknowledgements are not required for validity, but constitute prima facie evidence of the execution of an assignment, grant, or conveyance of a patent or patent application. 35 USC §261. The original or a true copy of the assignment document may be recorded in the USPTO. See 37 CFR §§3.1-3.41 for recording requirements. If there are two conflicting assignments, the one executed first prevails if it has been properly recorded within three months after execution or, in any event, before recordation of the later assignment. If the first executed assignment does not qualify, then the later assignment prevails if it is recorded first and if it has been taken in good faith for valuable consideration and without notice of the first assignment. 35 USC §261.

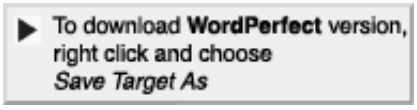
In §2.16 is an example of an assignment covering different types of intellectual property, including patents. The patent assignment should identify the patent by number and date, and also include the inventor and the title of the invention. A cover sheet as prescribed by the USPTO is required to be filed along with the assignment document. A copy of the cover sheet is reproduced in §2.17, and is available for downloading at http://www.uspto.gov/web/forms/pto1595.pdf.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/2 Patents and Trade Secrets/§2.16 2. Form: Patent Assignment

§2.16 2. Form: Patent Assignment





TRANSFER AND ASSIGNMENT OF INTELLECTUAL PROPERTY

This Transfer and Assignment of Intellectual Property Agreement (the "Agreement") is made and entered into as of _ _[*date*]_ _, by and between _ _[*name*]_ _ ("Assignor") and _ _[*name*]_ _ ("Assignee").

1. Assignor is the owner of the following items of intellectual property (the "Intellectual Property"): _ _[*Insert identifying information such as title and registration number for patents, trademarks, or copyrights, and description of trade secrets. Information must be complete and accurate. The information may be set forth in an exhibit.*]_ _

2. For good and valuable consideration, the receipt of which is hereby acknowledged _ _[*describe any other consideration*]_ _, Assignor hereby assigns, and transfers to Assignee, all of Assignor's interest in the Intellectual Property, together with all rights to secure registrations, renewals, reissues, and extensions of the copyrights, patents, and trademark rights included therein, if any.

3. Assignor hereby covenants, warrants, and represents to Assignee that:

(a) Assignor is the sole owner of and has the exclusive right to use the Intellectual Property, free and clear of any liens, encumbrances, licenses, or claims of any nature, and has made no agreement with respect to the Intellectual Property that is in conflict with this Agreement.

(b) Except as specified in Paragraph 1 of this Agreement, no other registration has been effected or is on file with the appropriate governmental agencies with respect to the Intellectual Property.

(c) If Assignor is an individual, Assignor agrees to authorize and direct his or her heirs and personal representatives to make and execute any instrument and perform any legal act that Assignee may deem necessary to secure the registration of, or any renewal or extension to, the registration of the Intellectual Property, as applicable.

(d) Assignor agrees to take such steps and make such filings as may be necessary or appropriate in the determination of Assignee to effect the transactions contemplated hereby.

4. This Agreement is governed by the laws of the State of California without regard to its conflict of law rules. This Agreement constitutes the entire agreement of the parties with respect to the subject matter hereof and may not be modified or amended without the written agreement of the parties.

IN WITNESS WHEREOF, the parties have executed this Agreement by their duly authorized representatives.

Assignor:

Date: _ _ _ _ _ _ _ _[*NAME OF ENTITY*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _
_ _[*Address*]_ _

Assignee:

Date: _ _ _ _ _ _ _ _[*NAME OF ENTITY*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _
_ _[*Address*]_ _

[*Insert Notarial Acknowledgment*]

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/2 Patents and Trade Secrets/§2.17 3. Form: U.S. Patent & Trademark Office Cover Sheet (Patents Only)

§2.17 3. Form: U.S. Patent & Trademark Office Cover Sheet (Patents Only)



Form **PTO-1595** (Rev. 01-09)
OMB No. 0651-0027 (exp. 02/28/2009)

U.S. DEPARTMENT OF COMMERCE
United States Patent and Trademark Office

RECORDATION FORM COVER SHEET
PATENTS ONLY

To the Director of the U.S. Patent and Trademark Office: Please record the attached documents or the new address(es) below.

1. Name of conveying party(ies)

Additional name(s) of conveying party(ies) attached? ☐ Yes ☐ No

2. Name and address of receiving party(ies)

Name: _____

Internal Address: _____

_____

Street Address: _____

_____

City: _____

State: _____

Country: _____ Zip: _____

Additional name(s) & address(es) attached? ☐ Yes ☐ No

3. Nature of conveyance/Execution Date(s):

Execution Date(s) _____

☐ Assignment ☐ Merger
☐ Security Agreement ☐ Change of Name
☐ Joint Research Agreement
☐ Government Interest Assignment
☐ Executive Order 9424, Confirmatory License
☐ Other _____

4. Application or patent number(s):

☐ This document is being filed together with a new application.

A. Patent Application No.(s)

B. Patent No.(s)

Additional numbers attached? ☐ Yes ☐ No

5. Name and address to whom correspondence concerning document should be mailed:

Name: _____

Internal Address: _____

_____

Street Address: _____

_____

City: _____

State: _____ Zip: _____

Phone Number: _____

Fax Number: _____

Email Address: _____

6. Total number of applications and patents involved: _____

7. Total fee (37 CFR 1.21(h) & 3.41) $ _____

☐ Authorized to be charged to deposit account
☐ Enclosed
☐ None required (government interest not affecting title)

8. Payment Information

Deposit Account Number _____

Authorized User Name _____

9. Signature:

_____ _____
Signature Date

_____
Name of Person Signing

Total number of pages including cover sheet, attachments, and documents: ☐

Documents to be recorded (including cover sheet) should be faxed to (571) 273-0140, or mailed to:
Mail Stop Assignment Recordation Services, Director of the USPTO, P.O.Box 1450, Alexandria, V.A. 22313-1450

Print

Guidelines for Completing Patents Cover Sheets (PTO-1595)

Cover Sheet information must be submitted with each document to be recorded. If the document to be recorded concerns both patents and trademarks separate patent and trademark cover sheets, including any attached pages for continuing information, must accompany the document. All pages of the cover sheet should be numbered consecutively, for example, if both a patent and trademark cover sheet is used, and information is continued on one additional page for both patents and trademarks, the pages of the cover sheet would be numbered from 1 to 4.

Item 1. Name of Conveying Party(ies).

Enter the full name of the party(ies) conveying the interest. If there is insufficient space, enter a check mark in the "Yes" box to indicate that additional information is attached. The name of the additional conveying party(ies) should be placed on an attached page clearly identified as a continuation of the information Item 1. Enter a check mark in the "No" box, if no information is contained on an attached page. If the document to be recorded is a joint research agreement, enter the name(s) of the party(ies) other than the owner of the patent or patent application as the conveying party(ies).

Item 2. Name and Address of Receiving Party(ies).

Enter the name and full address of the first party receiving the interest. If there is more than one party receiving the interest, enter a check mark in the "Yes" box to indicate that additional information is attached. Enter a check mark in the "No" box, if no information is contained on an attached page. If the document to be recorded is a joint research agreement, enter the name(s) of the patent or patent application owner(s) as the receiving party.

Item 3. Nature of Conveyance/Execution Date(s).

Enter the execution date(s) of the document. It is preferable to use the name of the month, or an abbreviation of that name, in order that confusion over dates is minimized. Place a check mark in the appropriate box describing the nature of the conveying document. If the "Other" box is checked, specify the nature of the conveyance.

Item 4. Application Number(s) or Patent Number(s).

Indicate the application number(s), and/or patent number(s) against which the document is to be recorded. National application numbers must include both the series code and a six-digit number (e.g., 07/123,456), and international application numbers must be complete (e.g., PCT/US91/12345).

Enter a check mark in the appropriate box: "Yes" or "No " if additional numbers appear on attached pages. Be sure to identify numbers included on attached pages as the continuation of Item 4. Also enter a check mark if this Assignment is being filed with a new application.

Item 5. Name and Address of Party to whom correspondence concerning the document should be mailed. Enter the name and full address of the party to whom correspondence is to be mailed.

Item 6. Total Applications and Patents involved.

Enter the total number of applications and patents identified for recordation. Be sure to include all applications and patents identified on the cover sheet and on additional pages.

Block 7. Total Fee Enclosed.

Enter the total fee enclosed or authorized to be charged. A fee is required for each application and patent against which the document is recorded.

Item 8. Payment Information.

Enter the deposit account number and authorized user name to authorize charges.

Item 9. Signature.

Enter the name of the person submitting the document. The submitter must sign and date the cover sheet. Enter the total number of pages including the cover sheet, attachments, and document.

This collection of information is required by 35 USC 261 and 262 and 15 USC 1057 and 1060. The information is used by the public to submit (and by the USPTO to process) patent and trademark assignment requests. After the USPTO records the information, the records for patent and trademarks, assignments, and other associated documents can be inspected by the public. To view documents recorded under secrecy orders or documents recorded due to the interest of the federal government, a written authorization must be submitted. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the form to the USPTO. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Manager of the Assignment Division, USPTO, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop Assignment Recordation Services, Director of the USPTO, P.O. Box 1450, Alexandria, VA 22313-1450.

Print

Privacy Act Statement for Patent Assignment Recordation Form Cover Sheet

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with the above request for information. This collection of information is authorized by 35 U.S.C. 1, 2, 261 and E.O. 9424. This information will primarily be used by the USPTO for the recordation of assignments related to patents and patent applications. Submission of this information is voluntary but is required in order for the USPTO to record the requested assignment. If you do not provide the information required on the cover sheet, the assignment will not be recorded, and all documents will be returned to you.

After the information is recorded, the records and associated documents can be inspected by the public and are not confidential, except for documents that are sealed under secrecy orders or related to unpublished patent applications. Assignment records relating to unpublished patent applications are maintained in confidence in accordance with 35 U.S.C. 122. Records open to the public are searched by users for the purpose of determining ownership for other property rights with respect to patents and trademarks.

Routine uses of the information you provide may also include disclosure to appropriate Federal, state, local, or foreign agencies in support of their enforcement duties and statutory or regulatory missions, including investigating potential violations of law or contract and awarding contracts or other benefits; to a court, magistrate, or administrative tribunal in the course of presenting evidence; to members of Congress responding to requests for assistance from their constituents; to the Office of Management and Budget in connection with the review of private relief legislation; to the Department of Justice in connection with a Freedom of Information Act request; to a contractor in the performance of their duties; to the Office of Personnel Management for personnel studies; and to the General Services Administration (GSA) as part of their records management responsibilities under the authority of 44 U.S.C. 2904 and 2906. Such disclosure to GSA shall not be used to make determinations about individuals.

© The Regents of the University of California

§2.17A I. Litigation Issues

The recent trend in case law has been to loosen impediments for litigants who are attacking the validity of a patent holder's claims or defending against a claim of patent infringement made by a patent holder. A key issue in *MercExchange, LLC v eBay, Inc*. (Fed Cir 2005) 401 F3d 1323, was whether the lower court properly refused to grant MercExchange a permanent injunction against eBay. The appellate court reversed the lower court's denial of a permanent injunction, finding that "the general rule is that a permanent injunction will issue once infringement and validity have been adjudged." 401 F3d at 1338. This presumption favoring issuance of a permanent injunction had been used as leverage against allegedly infringing manufacturers who would rather settle with litigants challenging the validity of their patents than risk seeing their product denied access to the market pending final resolution of the infringement action. The United States Supreme Court vacated and remanded the appellate court decision, holding that courts should not automatically issue a permanent injunction following a finding of patent infringement, but should instead apply traditional equitable principles when analyzing whether an injunction should issue. *eBay, Inc. v MercExchange, LLC* (2006) 547 US 388, 164 L Ed 2d 641, 126 S Ct 1837.

Continuing the trend, the Supreme Court held in *MedImmune, Inc. v Genentech* (2007) 549 US 118, 137, 166 L Ed 2d 604, 621, 127 S Ct 764, that a company does not have to terminate its patent license before bringing an action to invalidate the underlying patent. The prior rule required a licensee to terminate its license and cease paying royalties prior to bringing an action for invalidation, in which case a licensee that did not prevail on the invalidation claim would be liable as an infringer for treble damages.

A similar case is *In re Seagate Technol., LLC* (Fed Cir 2007) 497 F3d 1360, in which the court reviewed the standard for proving willful infringement, a requirement for an award of enhanced damages in an infringement case. The court held that a showing of "objective recklessness" is required to prove willful infringement, a departure from the prior rule requiring merely a showing that the defendant failed to "exercise due care" to determine if a product was infringing. 497 F3d at 1371.

© The Regents of the University of California

J. Special Topics for Internet Businesses

§2.18 1. Business Method Patents

A business method in its most generic form is a method of adding value to an existing product or service through a series of steps or processes. One example of a business method is a patent currently held by Priceline.com relating to auctions on the Internet. U.S. Patent Number 5,794,207, issued August 11, 1998, is entitled "Method and apparatus for a cryptographically assisted commercial network system designed to facilitate buyer-driven conditional purchase offers" and its abstract reads in part as follows:

> The present invention is a method and apparatus for effectuating bilateral buyer-driven commerce. The present invention allows prospective buyers of goods and services to communicate a binding purchase offer globally to potential sellers, for sellers conveniently to search for relevant buyer purchase offers, and for sellers potentially to bind a buyer to a contract based on the buyer's purchase offer. In a preferred embodiment, the apparatus of the present invention includes a controller which receives binding purchase offers from prospective buyers. The controller makes purchase offers available globally to potential sellers. Potential sellers then have the option to accept a purchase offer and thus bind the corresponding buyer to a contract. The method and apparatus of the present invention have applications on the Internet as well as conventional communications systems such as voice telephony.

On Priceline.com's website, consumers "name the price" they are willing to pay for airline tickets, using an auction format where the first willing seller gets the sale. This is a well known auction technique offline, but Priceline claims that the patent gives it the exclusive right to use this sales method on the Internet.

Prior to 1998, methods of doing business were not considered patentable subject matter. In 1996, the USPTO began to move away from its longstanding position with respect to business method patents, by removing from the USPTO, Manual for Patent Examining Procedure a reference to the 1908 case of *Hotel Sec. Checking Co. v Lorraine Co.* (2nd Cir 1908) 160 F 467, which had endorsed the business method exception to patentability. The Federal Circuit followed, affirmatively "lay[ing] this ill-conceived exception to rest" in *State St. Bank & Trust Co. v Signature Fin. Group* (1998) 149 F3d 1368, 1375, cert denied (1999) 525 US 1093. The Federal Circuit held that business methods should be subject to the same requirements for patentability as any other process. 149 F3d at 1377.

Following the *State St.* decision, the USPTO began receiving an increasing number of business method patent applications, including ones relating to the conduct of business on the Internet. See, *e.g., Amazon.com, Inc. v Barnes & Noble.com, Inc.* (Fed Cir 2001) 239 F3d 1343 (defendant allegedly infringed on plaintiff's patented "one-click" purchasing system; plaintiff denied preliminary injunction after defendant introduced evidence of prior art calling into question validity of plaintiff's patent).

Because business method patents are a relatively new phenomenon, it is not clear to what extent the USPTO will grant broad patents on business methods or, more importantly, to what extent the Federal Circuit will be willing to enforce infringement claims for such patents. More information about business method patents, including the guidelines used by the USPTO to examine them, is available at http://www.uspto.gov/web/menu/pbmethod.

Courts have generally enforced business method patents. In *MercExchange, LLC v eBay, Inc.* (ED Va 2003) 275 F Supp 2d 695, a federal jury found that online auction house eBay, Inc., and eBay's wholly owned subsidiary, Half.com, Inc., willfully infringed two business method patents owned by MercExchange. The jury awarded MercExchange $35 million in compensatory damages. The case related to the "Buy it Now" feature on eBay, which offers customers the option of buying an auction item at a fixed, preset price. On appeal, the Federal Circuit affirmed one of the two findings of patent infringement, reversed the other, and substantially reduced the damage award. *MercExchange, LLC v eBay, Inc.* (Fed Cir 2005) 401 F3d 1323, vacated on other grounds (2006) 547 US 946.

However, recent decisions appear to limit the eligibility of processes and business methods for patent protection. In *In re Bilski* (Fed Cir 2008) 545 F3d 943, 954, cert granted sub nom *Bilski v Doll* (2009) ___ US ___, 174 L Ed 2d 246, 129 S Ct 2735, the court held that a process or business method is eligible for patent protection only if it is tied to a particular machine or apparatus or transforms a particular article into a different state or thing. Applying the machine or

transformation test to Bilski's method for hedging commodities trading risk, the court found the process constituted unpatentable subject matter and described it as (545 F3d at 965):

> a non-transformative process that encompasses a purely mental process of performing requisite mathematical calculations without the aid of a computer or any other device, mentally identifying those transactions that the calculations have revealed would hedge each other's risks, and performing the post-solution step of consummating those transactions.

As a result of *Bilski*, patent protection for business methods may be more difficult to obtain. See also *In re Comiskey* (Fed Cir 2009) 554 F3d 967 (claims alleging novel way of ensuring arbitration of certain disputes comprised unpatentable mental process).

Practitioners should be aware that some basic practices on the Internet may be subject to patent protection and should take those issues into consideration in their review of their clients' prospective business plans. Some notable patents that relate to the Internet include:

- One-click online shopping (U.S. Patent No. 5,960,411);
- Online shopping carts (U.S. Patent No. 5,715,314);
- The hyperlink (U.S. Patent No. 4,873,662);
- Video streaming (U.S. Patent No. 5,132,992);
- Internationalizing domain names (U.S. Patent No. 6,182,148);
- Pop-up windows (U.S. Patent No. 6,389,458);
- Targeted banner ads (U.S. Patent No. 6,026,368);
- Paying with a credit card online (U.S. Patent No. 6,289,319); and
- Framed browsing (U.S. Patent Nos. 5,933,841 and 6,442,574).

© The Regents of the University of California

§2.19 2. Software Patents

Before 1994, computer software was widely believed to be unpatentable because it was considered as falling within the "mathematical algorithm" exception to patentable subject matter. See §2.3. The Supreme Court clarified that exception in *Diamond v Diehr* (1981) 450 US 175, 192, 67 L Ed 2d 155, 169, 101 S Ct 1048 (claim implementing mathematical formula in structure or process performing function that patent laws were designed to protect is patentable). In 1994, the Federal Circuit rejected the mathematical algorithm exception as applied to computer software, finding that the Supreme Court deemed unpatentable only "disembodied mathematical concept[s]." *In re Alappat* (Fed Cir 1994) 33 F3d 1526, 1544. The Federal Circuit held that when a mathematical algorithm is used as part of a "particularly claimed combination of elements" in a machine or process, it is patentable subject matter if it meets the other requirements for patentability. 33 F3d at 1544. See also *State St. Bank & Trust Co. v Signature Fin. Group* (1998) 149 F3d 1368, 1373, cert denied (1999) 525 US 1093 ("to be patentable an algorithm must be applied in a 'useful' way").

Both *Alappat* and *State Street* involved patent claims for machines that produced certain results. In *AT&T Corp. v Excel Communications, Inc.* (Fed Cir 1999) 172 F3d 1352, cert denied (1999) 528 US 946, the court clarified that the scope of patentable subject matter under 35 USC §101 is the same, holding that software by itself that produces a "useful, concrete and tangible result" is patentable as a process or method, despite the fact that it includes mathematical algorithms and it is not associated with particular hardware. 172 F3d at 1359. However, in *In re Bilski* (Fed Cir 2008) 545 F3d 943, 960, cert granted sub nom *Bilski v Doll* (2009) ___ US ___, 174 L Ed 2d 246, 129 S Ct 2735, the Federal Circuit held that the machine-or-transformation test was the proper test to apply in patent inquiries. 545 F3d at 959. The court rejected exclusive reliance on the "useful, concrete and tangible" test to determine patentability of a business method, abrogating *State Street* and *AT&T*. 545 F3d at 960 n10.

In one example of software patent enforcement, a jury awarded more than $520 million in damages to the University of California's Eolas Technologies, Inc. for infringement of a patent for technology that allows interactive applications such as "plug-ins" and "applets" to be embedded in Web pages. *Eolas Technols., Inc. v Microsoft Corp.* (ND Ill, Jan. 14, 2004, No. 99C0626) 2004 US Dist Lexis 534, aff'd in part and rev'd in part (Fed Cir 2005) 399 F3d 1325. On appeal, the case was remanded for retrial on the question of whether the patent owner, the University of California, knew of a prior invention that would allegedly invalidate the patent at issue. 399 F3d at 1333.

Plug-ins, applets, and similar programs covered by the University of California/Eolas patent are central to online commerce, because they enable services such as banner ads and interactive customer service. The implications of this case for the Internet are significant. Microsoft and other browser service providers are more likely to rewrite their programs than to continue shipping products and incur substantial license fees. A final victory for the University of California/Eolas could mean that web pages would have to be rewritten to work with the new browsers, causing widespread disruption of the Internet.

© The Regents of the University of California

II. TRADE SECRETS

§2.20 A. Introduction

The Internet allows people to disseminate and to obtain information quickly and easily, which may create problems for businesses trying to protect trade secrets. A trade secret is not protectible once it is generally known, either in the industry, by the public, or by others who can exploit its use. Information that is posted on a website is potentially accessible by anyone, including a company's competitors. If a trade secret is posted on the Internet, even for a very brief period of time, its status as a trade secret may be lost. See *Religious Technol. Ctr. v Netcom On-Line Communication Servs., Inc.* (ND Cal 1995) 923 F Supp 1231, 1255. Trade secrets are protected mainly by state law. The Uniform Trade Secrets Act (UTSA), which has been adopted by most states, sets forth the legal protections and remedies afforded to trade secret owners. With few modifications, California has codified the UTSA in its Civil Code, in CC §§3426-3426.11. For a comprehensive review of trade secret law in California, see Trade Secrets Practice in California (2d ed Cal CEB 1996).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/2 Patents and Trade Secrets/ B. Definition of Trade Secret/§2.21 1. Statutory Definition

B. Definition of Trade Secret

§2.21 1. Statutory Definition

The Restatement (Third) of Unfair Competition §39 (1993) defines a trade secret as:

> any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others.

Under California law (CC §3426.1(d)), a trade secret is similarly defined as:

> information, including a formula, pattern, compilation, program, device, method, technique, or process that:
> (1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and
> (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

© The Regents of the University of California

§2.22 2. Examples of Trade Secrets

Internet companies may find that significant elements of their intellectual property portfolio constitute important trade secrets that must be carefully monitored. Examples include customer lists, business plans, new product ideas, marketing strategies, know-how, and the non-public concepts and ideas behind a company's software and business models. In *Therapeutic Research Faculty v NBTY, Inc.* (ED Cal 2007) 488 F Supp 2d 991, 999, the federal district court ruled that the user name and passcode combination providing access to the plaintiffs' information constituted a trade secret having independent economic value. See generally Trade Secrets Practice in California §1.4 (2d ed Cal CEB 1996).

PRACTICE TIP: Any intellectual property protection strategy involves many considerations and should be carefully reviewed with experienced counsel.

© The Regents of the University of California

§2.22A 3. Computer Source and Object Code

Taking software as an example, the source and object code of a computer program may be protected by copyright (see §1.2), but the ideas of which the code is an expression are not. See 17 USC §102. The ideas themselves—the concept of what the software does and how it works—might be protected by patent or by trade secret law. Patents have significant advantages in that they grant the inventor the sole right to exploit the invention. The patent application process is costly, however, and may not be feasible for start-up companies without sufficient funding. Moreover, patent law requires the owner to describe the invention in detail on a patent application, and an issued patent is a public document. See 35 USC §§9-10, 111. Patents are issued for only 20 years (35 USC §154(a)(2)), while trade secrets are protectible for an unlimited period of time. Some intellectual property owners therefore prefer trade secret protection.

In *Viacom Int'l Inc. v YouTube Inc*. (SD NY 2008) 253 FRD 256, the federal district court ruled that the owners and operators of the video-sharing website YouTube were entitled to a protective order to prevent disclosure of the computer source code for the website's search function on the grounds that the source code was protectible as a trade secret.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/2 Patents and Trade Secrets/§2.22B 4. Recipes, Manufacturing Processes

§2.22B 4. Recipes, Manufacturing Processes

Recipes for famous beverages and foods, such as Coca-Cola, are prime examples of intellectual property rights that are better protected as trade secrets. Patenting the recipe would mean that the recipe would fall into the public domain on expiration of the patent term. Of course, if the recipe is stolen and publicized, it will lose trade secret protection.

© The Regents of the University of California

§2.23 5. Customer Lists

Customer lists are another example of a protectible trade secret. If the customer list is readily ascertainable, however (*e.g.*, by having been derived from the "yellow pages" or a trade directory), then trade secret protection may not be available. In *Greenly v Cooper* (1978) 77 CA3d 382, 392, 143 CR 514, the court explained that a list of customers or subscribers "built up by ingenuity, time, labor and expense of the owner over a period of many years is property of the employer." Factors that support a finding that a customer list is a trade secret are as follows (*Courtesy Temporary Serv., Inc. v Camacho* (1990) 222 CA3d 1278, 272 CR 352):

- Whether the business invested money in developing and maintaining the customer list;
- Whether the list contained particular and specific information about the customers; and
- The time and effort spent in acquiring the list.

For further discussion of customer lists, see Trade Secrets Practice in California §1.5 (2d ed Cal CEB 1996).

© The Regents of the University of California

§2.24 C. Loss of Trade Secret Protection

To retain trade secret protection, the trade secret must remain confidential. The Ninth Circuit in *Chicago Lock Co. v Fanberg* (9th Cir 1982) 676 F2d 400, 404, explained that "trade secrets do not enjoy the absolute monopoly protection afforded patented processes, for example, and trade secrets will lose their character as private property when the owner divulges them or when they are discovered through proper means." Similarly, in *Sinclair v Aquarius Electronics, Inc.* (1974) 42 CA3d 216, 116 CR 654, the court stated that a trade secret is not protected from discovery by fair and honest means (such as accidental discovery and reverse engineering). According to the *Sinclair* court, reverse engineering occurs when one "[starts] with the known product and [works] backward to divine the process." 42 CA3d at 226. As the *Chicago Lock* court explained, reverse engineering does not violate trade secret law because the act of reverse engineering is viewed as discovering a trade secret through fair means. A trade secret owner may try to prevent reverse engineering through a license, user, or nondisclosure agreement that restricts such action. For further discussion of reverse engineering, see Trade Secrets Practice in California §1.13 (2d ed Cal CEB 1996).

© The Regents of the University of California

§2.25 D. Protection of Trade Secrets

To maintain protection, companies need to take affirmative steps to preserve the secrecy of their trade secrets. Depending on the nature of the trade secret being protected, different measures may be used to achieve protection. As a starting point, a company must be able to identify its trade secrets. Thus, a policy of identifying and reporting on important trade secrets within the enterprise is a first step in any trade secret protection program. A nondisclosure agreement should be entered into with every individual who has access to the trade secret. (A form is provided in §2.33.) In addition, companies should implement a policy that sets forth guidelines for the treatment of trade secrets by employees and others who have access to them (such as independent contractors). A sample company policy is set forth in §2.31. See also Wilka, *How to Avoid Liability and Protect Trade Secrets When Hiring and Losing Employees*, 24 CEB Cal Bus L Prac 137 (Winter 2009); Trade Secrets Practice in California, chap 4 (2d ed Cal CEB 1996).

© The Regents of the University of California

§2.26 1. Departing Employees

Because employees are important repositories of a technology company's trade secrets and know-how, when employees leave their employment there is an opportunity for trade secrets to "walk out the door" with them. If the trade secret was not adequately documented or communicated to other company employees before the employee's departure, the enterprise will not have access to the information once the employee leaves. If employees do not understand their obligations of confidentiality to the employer, they may make inappropriate disclosures of company trade secrets after their departure to a subsequent employer or customer. On the departure of an employee with access to a company's trade secrets, the employer should conduct an exit interview with the departing employee to reiterate the company's policies and the legal consequences of disclosing the trade secrets to anyone. Part of the exit interview should confirm that all important know-how and trade secrets that the employee has generated or used during his or her employment are either known to other company employees or well documented. For suggested topics to cover in the exit interview and other procedures for departing employees, see section III.A.3 of the sample company policy set forth in §2.33. See also Wilka, *How to Avoid Liability and Protect Trade Secrets When Hiring and Losing Employees,* 24 CEB Cal Bus Law Prac 1 (Winter 2009); Trade Secrets Practice in California, chaps 4-6 (2d ed Cal CEB 1996).

No doctrine of inevitable disclosure in California. Some jurisdictions outside California apply a doctrine called "inevitable disclosure" to permit companies to stop former employees from using trade secrets of their former employer. See generally *PepsiCo, Inc. v Redmond* (7th Cir 1995) 54 F3d 1262; Trade Secrets Prac §12.13. Under this doctrine, grounds for trade secret misappropriation (and issuance of an injunction) may be found if a former employee is placed in a new employment position where disclosure of the former employer's trade secrets may be inevitable. See *Merck & Co. Inc. v Lyon* (MD NC 1996) 941 F Supp 1443, 1460. The doctrine of inevitable disclosure has never been the law in California. *Whyte v Schlage Lock Co.* (2002) 101 CA4th 1443, 125 CR2d 277. In *Whyte*, the court explained that the doctrine is not enforceable in California because it is essentially a covenant not to compete, and "California public policy strongly favors employee mobility." 101 CA4th at 1462. See also *Danjaq, LLC v Sony Corp.* (CD Cal Mar. 11, 1999, CV-978414-ER) 1999 US Dist Lexis 22486; *Bayer Corp. v Roche Molecular Sys., Inc.* (ND Cal 1999) 72 F Supp 2d 1111.

Non-compete covenants of limited enforceability in California. California is one of the minority of states that prohibit postemployment covenants not to compete, except in very limited situations. See Trade Secrets Prac §6.21. In the absence of a statutory exception (see Bus & P C §§16601-16602.5), the general rule is that "every contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void." Bus & P C §16600. See *VL Sys., Inc. v Unisen, Inc.* (2007) 152 CA4th 708, 61 CR3d 818. This general rule is subject to several statutory exceptions, but there is no "narrow restraint" or general reasonableness exception that courts may apply. *Edwards v Arthur Andersen LLP* (2008) 44 C4th 937, 949, 81 CR3d 282. In *Edwards,* the court reserved without deciding the question of "the applicability of the so-called trade secret exception to §16600." 44 C4th at 946 n4.

PRACTICE TIP: Consider including in employee confidentiality agreements a clause affirmatively acknowledging that the employer is permitted to contact an individual's subsequent employers to inform them of the employee's obligations not to divulge the trade secrets of its former employer, and inform the new employer that the employee is bound by a nondisclosure agreement. This puts the new employer on notice that the employee knows a protectible trade secret that cannot be used or accessed by the new employer. Some employers also include in their employee confidentiality agreements a provision requiring the employee to inform subsequent employers of such ongoing confidentiality obligations on the part of the employee.

© The Regents of the University of California

2. Practical Safeguards

§2.27 a. Firewalls and Encryption

A company doing business on the Internet should consider establishing technical safeguards to preserve confidentiality and restrictions on network access to demonstrate that the company has taken reasonable measures to protect its trade secrets. Conforming with industry standards of technical data security will aid counsel in any future trade secret protection lawsuits by evidencing that reasonable measures have been taken to preserve the secrecy of such information, as required by CC §3426.1(d). Firewalls should be placed between networks that send and receive trade secrets, as well as within networks that contain trade secrets. Firewalls are programs that (1) are located at a network gateway server, (2) protect information of a network from unauthorized users of other networks, and unauthorized users within the same network, and (3) are typically used to filter or block Internet addresses that do not have access to a particular website or area within a website. Information that is transmitted on the Internet should also be encrypted, so that persons outside the company cannot access the trade secret. Password protection for network access, as well as separate passwords for highly confidential documents, should also be in place. Trade secret data should not be posted on a company's website unless it is placed on a secure, password-protected page or section within the website accessible only by those who are bound by a confidentiality agreement.

NOTE: Companies doing business on the Internet should consider the use of encryption technologies to protect highly sensitive data.

© The Regents of the University of California

§2.28 b. Physical Security

If the nature of a company's business and intellectual property position merits it, companies should consider restricting access to their facilities, using log-in sheets and access cards, security systems, and security cameras. Such measures are not necessarily effective in preventing trade secret misappropriation, but may serve as a deterrent and may also provide important evidence of employee activities in the event of a lawsuit.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/2 Patents and Trade Secrets/§2.29 c. Managing Documents and Files

§2.29 c. Managing Documents and Files

Systematically marking important trade secret documents as "Confidential and Proprietary Information of XYZ Company" may serve to put employees on notice of the sensitive nature of the materials and the need to restrict disclosure to third parties.

© The Regents of the University of California

E. Sample Company Policy on Trade Secret Protection

§2.30 1. Introduction

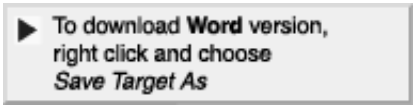
The following sample company policy integrates the protective measures discussed in §§2.25-2.29. This example is a highly detailed policy that may not be appropriate for all companies. Even the smallest technology company, however, may find that its most valuable assets are know-how and trade secrets. Many companies underestimate the value of intellectual property and thus do not take adequate steps to protect it. It is important to keep in mind, however, that if a policy is adopted but not followed, the failure to follow the policy may provide a tool for opposing counsel in litigation. Review any policy carefully before implementation to assess the company's practical ability to comply with it.

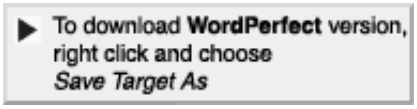
The drafter should consider adding a list of examples (either as an exhibit or in section II.A of the form in §2.31) of the company's trade secrets, such as engineering information, know-how, supplier lists, customer lists, business information, computer programs, pending patent applications, financial information, business plans, budgets, methods of calculating costs and pricing, internal marketing data, specifics concerning customers and suppliers, and collections of data, research, and other information regarding the company's business. The list of potential trade secret information should be reviewed in each case and conformed to the type of business the company is in, as well as to the types of business partners the company may have.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/2 Patents and Trade Secrets/§2.31 2. Form: Company Policy on Trade Secret Protection

§2.31 2. Form: Company Policy on Trade Secret Protection





POLICY FOR THE PROTECTION OF TRADE SECRETS AND CONFIDENTIAL INFORMATION OF _ _[*COMPANY NAME*]_ _

I. APPLICABILITY OF THIS POLICY. It is the policy of _ _[*name of company*]_ _ (the "Company") to comply fully with all applicable trade secret laws and to respect the trade secrets of others. The Company also owns trade secrets and takes appropriate steps to protect them. This manual contains the Company's policies and procedures relating to its own trade secrets and those of others. Such policies and procedures apply to all officers, full-time and part-time employees, independent contractors, consultants, and agents of the Company.

II. DEFINITION AND IDENTIFICATION OF TRADE SECRETS AND CONFIDENTIAL INFORMATION

A. DEFINITION OF TRADE SECRETS AND CONFIDENTIAL INFORMATION

1. DEFINITION OF TRADE SECRETS. For information to qualify as a trade secret, it must not be generally known to the public or to persons outside of the Company who are knowledgeable about the general subject matter of the information. Combinations of nonsecret elements also can be trade secrets. Trade secret information also must confer an actual or potential economic or business advantage on one who possesses the information. We treat as trade secrets all Company information not generally known outside of the Company that confers a potential business advantage on us, unless (a) such information is already protected by another means (such as by copyright or patent), or (b) treating it as secret would conflict with any other form of intellectual property protection.

All Company officers, managers, directors, and supervisors should regularly assess all of the Company's information within their purview to identify what information should be identified and maintained as trade secrets, and to take appropriate steps (as outlined in this Policy) to maintain the secrecy of such information. We err on the side of maintaining the secrecy of Company information. If you are unsure whether certain information should be treated as a trade secret or have questions about the appropriate efforts to maintain the secrecy of any information, please contact the Legal Department.

2. DEFINITION OF CONFIDENTIAL INFORMATION. All trade secrets are confidential information, but business information that may not rise to the level of a trade secret also may be deemed confidential within the Company. This includes any documents or physical objects marked as confidential, categories of documents and objects designated as confidential, physical areas designated as confidential, and any other information, objects, locations, and similar items that the Company wishes to treat as confidential by any means. Questions as to whether certain information should be treated as confidential should be directed to the Legal Department _ _[*or name of person or title*]_ _.

B. IDENTIFICATION OF TRADE SECRETS AND CONFIDENTIAL INFORMATION

1. DOCUMENTATION OF TRADE SECRETS. We document trade secrets whenever possible. All Company officers, managers, directors, and supervisors should assure that all trade secrets are documented in paper or electronic form. Questions regarding whether or how to document trade secret information should be directed to the Legal Department.

2. NOTICE OF CONFIDENTIALITY AND MARKING OF DOCUMENTS. All trade secrets must be accompanied by a notice of confidentiality or be marked or designated as confidential information. The following notice must be stamped or otherwise applied to the first or main title page of all trade secret documents in either paper or electronic form:

CONFIDENTIAL

This document contains trade secrets or otherwise confidential information owned by _ _[*name*]_ _. Access to and use of this information is strictly limited in accordance with the Policy for the Protection of Trade Secrets and Confidential Information of _ _[*name*]_ _ (the "Policy"). This document may not be distributed or otherwise disclosed outside of _ _[*name*]_ _'s facilities except under appropriate precautions to maintain the confidentiality of the document, and may not be used in any way not expressly authorized by the Policy.

The words "Confidential Information of _ _[*name*]_ _" must be stamped or otherwise applied to all other pages of such trade secret documents.

When trade secrets cannot be documented, they must be accompanied by a notice of confidentiality or otherwise designated as confidential by a method appropriate under the circumstances. For example, physical facilities containing or constituting trade secrets may be designated as confidential by posting appropriate signs or placing appropriate labels on hardware. As another example, electronic media, e-mails, or electronic files containing trade secrets should bear or be accompanied by an appropriate notice of confidentiality. The following is a sample notice of confidentiality that should be modified as appropriate under the circumstances:

CONFIDENTIAL

This equipment contains trade secrets or other confidential information owned by _ _[*name*]_ _. _ _[Or: *"Trade secrets or other confidential information owned by _ _[name]_ _ are used in this area."*]**_ _ Access to and use of this information is strictly limited in accordance with the company's Policy for the Protection of Trade Secrets and Confidential Information (the "Policy"). This information may not be disclosed outside of _ _[*name*]_ _'s facilities except under appropriate precautions to maintain the confidentiality of the information, and may not be used in any way not expressly authorized by the Policy.**

Questions regarding whether or how to mark or otherwise designate documents or other information as trade secrets should be directed to the Legal Department _ _[*or name of person or title*]_ _.

III. PRESERVATION OF TRADE SECRETS AND OTHER CONFIDENTIAL INFORMATION

A. PROTECTION OF TRADE SECRETS IN RELATIONS WITH EMPLOYEES

1. EMPLOYEE OBLIGATIONS. As a condition of initial or continued employment, all employees must sign an employment application _ _[*or separate employee confidentiality agreement*]_ _ setting forth their obligations with respect to the Company's trade secrets and other matters. We enforce such agreements to the fullest extent of the law, but our failure to do so in any particular instance will not waive or otherwise affect the Company's right or ability to enforce the provisions of another agreement in any other instance.

The Company may change its employment application _ _[*or standard employee confidentiality agreement*]_ _ from time to time. Accordingly, this Policy may change from time to time as the employment application _ _[*or employee confidentiality agreement*]_ _ is changed. Thus, an employee's obligations with respect to trade secrets (or other matters) may be broader or different than as set forth in the employment application signed by the employee at an earlier time. As a condition for continued employment, and to reduce uncertainty regarding the employee's obligations at any particular time, the Company may require employees to execute an acknowledgment of their trade secret obligations or other obligations from time to time.

2. PROCEDURES FOR ARRIVING EMPLOYEES. All new employees must sign the Company's standard employment agreement, which may change from time to time. A designee of the Human Services Department will meet with each arriving employee within five (5) working days after the commencement of the employee's employment. That person must:

a. Explain this Policy to the employee and give the employee a copy of this Policy.

b. Ask the employee if he or she retained any information that may be a trade secret or confidential information of his/her prior employer(s) after leaving such employment.

c. Ascertain the nature and subject matter areas of the work performed by the employee for prior employers (but instruct the employee not to reveal any trade secrets or confidential information of any prior employer when answering this question).

d. Inform the employee that under certain circumstances the Company may need to contact the employee's

former employer(s) regarding the scope of the employee's obligations to his/her former employer(s) or regarding the employee's answers or comments to items b and c above.

e. Instruct the employee that he or she may not use or bring into the Company's facilities or computers (by any means) any information, documents, or physical objects learned or obtained from any prior employer or considered to be proprietary by any other person.

f. Ask the employee to confirm that he or she understands the matters discussed under items a through e above.

g. During the meeting, prepare a report documenting the discussion with the employee and his/her answers and comments regarding items a through f above.

If the employee (1) answers affirmatively to item b above and will be performing substantially the same type or nature of work or will be working in substantially the same subject matter areas for the Company as for any prior employer, or (2) disagrees with any of the matters discussed under items a-e above, the person conducting the interview must immediately contact the Legal Department after the consultation. The Company's policy is to contact an employee's former employer(s) when, in the judgment of the appropriate officer of the Company and the Legal Department, such contact is likely to reduce the risk of a dispute between the Company and any employee's former employer(s).

3. PROCEDURES FOR DEPARTING EMPLOYEE. Appropriate personnel from the Human Services Department will meet with each departing employee no more than _ _[*number*]_ _ working days before the employee's last day of employment (unless an employee departs the Company without notice). In that meeting, the Human Services personnel must:

a. Inform the employee that he or she has various obligations to the Company that survive the termination of employment, such as the employee's trade secret obligations and any other obligations as set forth set forth in his/her employment agreement _ _[*or employee confidentiality agreement, or employment application*]_ _.

b. Ask the employee the nature and subject matter areas of the work expected to be performed for his/her next employer (but instruct the employee not to reveal any trade secrets or confidential information of his/her next employer when answering this question).

c. Inform the employee that under certain circumstances the Company may need to advise the employee's next employer of the employee's obligations under his/her employment agreement with the Company.

d. Instruct the employee that he or she may not use or bring into any future employer's facilities or computers (by any means) any information, documents, or physical objects learned or obtained from the Company or considered to be proprietary by any other person to which the Company has any legal obligations.

e. Remind the employee that the Company may, without prior notice, take legal action against the employee and/or his/her future employers for using or bringing into any future employer's facilities or computers (by any means) any specific information, documents, or physical objects learned or obtained from the Company or considered to be proprietary by any other person to which the Company has any legal obligations.

f. Ask the employee to identify the information, documents, or physical objects (including computer programs, manuals, or design documentation) that the employee plans on retaining after leaving the Company's employment.

g. Confirm that the employee understands the matters discussed under items a through f above.

h. During the meeting, prepare a report documenting the discussion with the employee and his/her answers and comments regarding items a through g above.

If the employee (1) answers affirmatively to item b above and will be performing substantially the same nature of work or will be working in substantially the same subject matter areas for his/her next employer as for the Company, or (2) disagrees with any of items a through g above, the person conducting the interview must contact the Legal Department immediately so that appropriate action can be taken. We will contact an employee's next employer when, in the judgment of the appropriate officer of the Company and the Legal

Department, such conduct is likely to reduce the risk of a dispute between the Company and any employee's next employer, or when such contact appears to be necessary to reduce the risk that the employee and/or his/her next employer will learn or use any Company trade secrets.

4. SPEECHES AND TECHNICAL PAPERS. The presentation of any speeches or technical papers containing any trade secrets by any employees to any person(s) not under an obligation of confidentiality to the Company must be authorized in advance in writing by an officer of the Company. This pre-clearance is required to: (a) prevent an inadvertent disclosure of trade secrets; (b) provide the opportunity for a review of the technical accuracy of papers or speeches; and (c) provide the time and opportunity to prepare and file patent applications, if appropriate, before the information set forth in such speeches or papers is disclosed to the public.

If any such speeches or papers relate to the subject matter of any joint venture between the Company and any other entity, or include any information that may be considered proprietary to any other entity, the Company officer or designated employee with authority over such trade secrets must contact the Legal Department before the presentation is made.

5. INTERNAL SECURITY MEASURES. All Company officers, managers, directors, and supervisors should assure that the following security measures are instituted and followed, as appropriate, with respect to all trade secrets. Questions regarding which security measures should be used in any particular circumstances, how to follow and enforce such security measures, and how to respond to breaches of such security measures should be directed to the Legal Department _ _[*or name of person or title*]_ _.

a. Materials containing trade secrets must be stored and handled with sufficient care to maintain their confidentiality. Trade secret information not reduced to documented form must be maintained with sufficient care to maintain its confidentiality.

b. Documents, physical objects, and undocumented information (such as processes) containing or constituting trade secrets must not be left in plain view and must not be accessible to any persons (particularly nonemployees, such as visitors) who are not authorized to have access thereto and who have not signed an agreement with the Company containing appropriate confidentiality obligations to the Company.

c. Documents containing trade secrets must be maintained in secure locations, under lock and key when possible, when not in use and after business or work hours.

d. When appropriate, a finite number of copies of such documents should be maintained, and authorized persons accessing such copies should be required to sign them out, sign them in, not make any copies, and maintain access only for a finite period of time.

e. Trade secret information stored in computers or in magnetic media must be password or copy protected and/or encrypted, and must not be accessible to unauthorized persons or through the Internet, e-mail, or any other form of electronic communication.

f. Employees must be reminded periodically of their confidential obligations under this Policy and as a condition of their employment. Such reminders must be made no less than twice annually.

g. Unneeded copies, whether electronic or paper, containing trade secrets should be destroyed.

h. Visitors to the Company's facilities must be required to sign in and to sign out, must be escorted by a Company employee at all times, and must be required to wear "Visitor" badges. Company employees with authorized access to secret areas may not take visitors to such areas unless such visitors have executed an appropriate confidentiality agreement.

i. Trade secrets must not be disclosed to any person owing no obligations of confidentiality to the Company.

j. Employees may not download or otherwise transmit trade secrets to their home computers, remove materials containing trade secrets from the Company premises, or disclose trade secrets to persons under an obligation of confidentiality to the Company except with prior, express, written permission of an officer or designated employee of the Company with authority over such trade secrets.

6. LIMITED ACCESS TO TRADE SECRETS. Only employees who need to know a trade secret for purposes of carrying out their employment duties may have access to such trade secret. All Company officers, managers, directors, and supervisors should ensure that trade secrets are accessible only to employees with such need to know them, and only to the extent necessary for such employees to carry out their duties. Access should be appropriately limited to the particular materials containing the information the employee needs to know.

B. PROTECTION OF TRADE SECRETS IN RELATIONS WITH NONEMPLOYEES

1. PLANT SECURITY AND PROCEDURES FOR VISITORS. See section III.A.5 (Internal Security Measures).

2. AGREEMENTS WITH INDEPENDENT CONTRACTORS. As a condition of initial or continued engagement, all independent contractors must sign an agreement setting forth the contractor's obligations with respect to the Company's trade secrets and other matters.

The terms of the Company's independent contractor agreements are part of this Policy. The Company may change such agreements from time to time, and this Policy may change from time to time as the agreements are changed. Thus, a contractor's obligations with respect to trade secrets (or other matters) may be broader or different than as set forth in the contractor agreement signed by the contractor at an earlier time. As a condition for continued engagement, and to reduce uncertainty regarding the contractor's obligations at any particular time, the Company may require contractors to execute the Company's current contractor agreement from time to time.

3. AGREEMENTS WITH OTHER COMPANIES. Trade secrets may not be disclosed to persons or entities other than Company employees or independent contractors who have given appropriate employment or other covenants, unless such persons or entities sign an appropriate confidential disclosure agreement or other agreement containing sufficient confidentiality obligations to the Company. Such agreements must be prepared and/or approved by the Legal Department. The obligations of recipients of trade secrets under such agreements shall be perpetual unless the trade secrets become publicly known through no act or omission of the recipients.

© The Regents of the University of California

F. Confidentiality Agreement

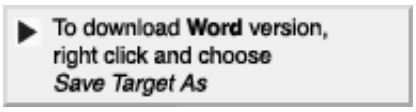
§2.32 1. Introduction

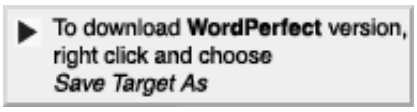
In §2.33 is a model form of mutual nondisclosure agreement to be entered into between two independent parties who are investigating the possibility of working together on a transaction or in another type of business relationship. Note that this form requires that sensitive information be marked "confidential" to be afforded protection under the agreement. Businesses should consider carefully whether imposing such a requirement would be beneficial. Marking requirements serve to more clearly identify the confidential information being transmitted and should aid significantly in subsequent litigation. If a marking requirement is not complied with, however, the business runs the risk that none of the unmarked information will be protected under the agreement.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/2 Patents and Trade Secrets/§2.33 2. Form: Confidentiality Agreement

§2.33 2. Form: Confidentiality Agreement





MUTUAL NONDISCLOSURE AGREEMENT

This Mutual Nondisclosure Agreement (the "Agreement") is entered into as of _ _[*date*]_ _, (the "Effective Date"), by and between _ _[*name*]_ _ and _ _[*name*]_ _ (collectively, the "Parties," and each a "Party").

WHEREAS, the Parties have certain confidential information relating to their respective businesses and to the subject area of _ _[*describe subject*]_ _, which they desire to disclose to each other for the purpose of exploring a possible business relationship between them _ _[*describe proposed relationship, if possible*]_ _, and each Party is willing to accept the other's information confidentially subject to the terms of this Agreement.

NOW THEREFORE, in consideration of the mutual covenants and agreements contained herein and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. DEFINITION OF CONFIDENTIAL INFORMATION. As used in this Agreement, "Confidential Information" means any confidential or proprietary information disclosed or made available by one Party (the "Discloser") to the other Party (the "Recipient") that is marked "confidential" or "proprietary" before its disclosure. In addition, information that is orally disclosed by the Discloser to the Recipient shall be Confidential Information if it is identified as such by the Discloser at the time of its disclosure and if, within fifteen (15) business days after disclosure, the Discloser delivers to the Recipient a written document describing such Confidential Information in detail, referencing the place and date of such oral disclosure and the name of the agents of the Recipient receiving such oral information, and stating that such information is deemed confidential by the Discloser.

2. EXCEPTIONS TO DEFINITION OF CONFIDENTIAL INFORMATION. Notwithstanding any other provision of this Agreement, each Party acknowledges that Confidential Information shall not include any information that the Recipient can demonstrate (a) was publicly available at the time of disclosure, or later became publicly available through no act or omission of the Recipient; (b) was already in Recipient's possession at the time of disclosure; (c) was rightfully received by the Recipient from a third party without any obligation of confidentiality; or (d) was independently developed by or for the Recipient without use of Discloser's Confidential Information.

3. USE OF CONFIDENTIAL INFORMATION. The Recipient shall use Discloser's Confidential Information only for the purpose of internal evaluation of and collaboration with the Discloser on the proposed business relationship, and shall make no use of Discloser's Confidential Information, in whole or in part, for any other purposes. The Recipient agrees to refrain from disclosing Discloser's Confidential Information to third parties, unless the Discloser has given its prior written authorization. The Recipient further agrees to keep confidential all of Discloser's Confidential Information and to take all reasonable steps to preserve the confidential and proprietary nature of such Confidential Information.

4. REQUIRED DISCLOSURE. If the Recipient is requested or required by subpoena or other court order to disclose any of Discloser's Confidential Information, the Recipient shall provide immediate notice of such request to the Discloser and shall use reasonable efforts to resist disclosure, until an appropriate protective order may be sought, or a waiver of compliance with the provisions of this Agreement is granted. If, in the absence of a protective order or the receipt of a waiver under this Agreement, the Recipient is nonetheless, in the written opinion of its counsel, legally required to disclose Discloser's Confidential Information, then, in such event, the Recipient may disclose such information without liability under this Agreement, provided that the Discloser has been given a reasonable opportunity to review the text of such disclosure before it is made and that the disclosure is limited to only the Confidential Information specifically required to be disclosed.

5. RETURN OF CONFIDENTIAL INFORMATION. The Discloser may elect at any time to terminate further

access to its Confidential Information. On written request, the Recipient shall return to the Discloser all Confidential Information in any form and promptly destroy any and all material or information derived from the Confidential Information, including any copies, except that one copy of the same may be retained for archival and evidence purposes only.

6. TERM. Regardless of the termination of any business relationship or negotiations between the Parties, this Agreement and the obligations of confidentiality and nondisclosure contained in it shall remain in full force and effect for _ _[*number*]_ _ years after the Effective Date, or such longer time as the Parties may agree in writing.

7. REMEDIES FOR BREACH OF AGREEMENT. The Confidential Information protected by this Agreement is of a special character, such that money damages would not be sufficient to avoid or compensate for any unauthorized use or disclosure of the Confidential Information. The Parties agree that injunctive and other equitable relief would be appropriate to prevent any such actual or threatened unauthorized use or disclosure. The remedies stated above may be pursued in addition to any other remedies available at law or in equity,

[*If appropriate, add*]

and the Recipient agrees to waive any requirement for the securing or posting of any bond in connection with such remedy.

[*Continue*]

In the event of litigation to enforce any provision of this Agreement, the prevailing Party shall be entitled to recover all costs, including its reasonable attorney fees and costs, incurred in connection with the litigation.

8. NO OTHER AGREEMENT. This Agreement is not and shall not be construed as any form of a letter of intent or agreement to enter into any type of transaction. This Agreement is to evidence the Parties' agreement to maintain the confidentiality of the Confidential Information, and shall not constitute any commitment or obligation on the part of either Party to enter into any specific contractual arrangement of any nature whatsoever.

9. NO REPRESENTATIONS. The Discloser does not make any representations or warranties as to the accuracy, completeness, or fitness for a particular purpose of any information disclosed to the Recipient under this Agreement. Neither the Discloser nor its representatives shall have any liability or responsibility to the Recipient (except as provided in this Agreement) or to any other person or entity resulting from the use of any information so furnished or otherwise provided.

10. GOVERNING LAW. California law shall govern the interpretation of this Agreement, without reference to rules regarding conflicts of law. Any dispute arising out of this Agreement shall be submitted to a state or federal court sitting in _ _[*city and state*]_ _, which shall have the exclusive jurisdiction regarding the dispute and to whose jurisdiction the Parties irrevocably submit.

11. NO WAIVER. No waiver of any term, provision, or condition of this Agreement, whether by conduct or otherwise, in any one or more instances, shall be deemed to be or be construed as a further or continuing waiver of any such term, provision, or condition or as a waiver of any other term, provision, or condition of this Agreement.

12. SEVERABILITY. If any provision of this Agreement is determined by any court of competent jurisdiction to be invalid or unenforceable, such provision shall be interpreted to the maximum extent to which it is valid and enforceable, all as determined by such court in such action, and the remaining provisions of this Agreement shall, nevertheless, continue in full force and effect without being impaired or invalidated in any way.

13. ENTIRE AGREEMENT. This Agreement constitutes the Parties' entire Agreement with respect to the subject matter hereof and supersedes any and all prior statements or agreements, both written and oral. This Agreement may not be amended except by a writing signed by the Parties.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed by their duly authorized representatives.

Date: _ _ _ _ _ _

_ _[*NAME OF ENTITY*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: _ _[*Signature*]_ _
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _
_ _[*Address*]_ _

Date: _ _ _ _ _ _

_ _[*NAME OF ENTITY*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: _ _[*Signature*]_ _
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _
_ _[*Address*]_ _

© The Regents of the University of California

G. Misappropriation of Trade Secrets

§2.34 1. Asserting Claim of Misappropriation Under UTSA

To assert a misappropriation claim in California under the Uniform Trade Secrets Act (UTSA) (CC §§3426-3426.11), the plaintiff must prove that (1) the trade secret has actual or potential economic value that is derived from not being generally known to the public or to persons who can obtain an economic advantage from its disclosure or use; (2) reasonable efforts were taken to maintain the secrecy of the trade secret; and (3) the trade secret was misappropriated. See generally Trade Secrets Practice in California §§1.11-1.12 (2d ed Cal CEB 1996).

If a trade secret has not been misappropriated, but misappropriation is threatened, the person who may potentially misappropriate the trade secret may be enjoined from doing so under CC §3426.2(a). In that case, the injunction would only last until the trade secret ceases to exist or, on request to the court, for a longer period of time.

© The Regents of the University of California

§2.35 2. Defenses

There are several defenses to a claim of misappropriation. One is that the defendant gained access to the trade secret by reverse engineering, which is lawful in most states, or gained access to the trade secret through other fair and lawful means under *Chicago Lock Co. v Fanberg* (9th Cir 1982) 676 F2d 400. See §2.24; Trade Secrets Practice in California §§1.13-1.14 (2d ed Cal CEB 1996). Another defense is that the trade secret was divulged by its owner and thus is no longer a trade secret under *Sinclair v Aquarius Electronics, Inc.* (1974) 42 CA3d 216, 116 CR 654. See §2.24. A person who downloads from the Internet a trade secret that was misappropriated by the person who posted it on the Internet may defend a misappropriation lawsuit if the defendant did not know that the information was misappropriated. A person who simply downloads misappropriated information is probably not liable. See *Religious Technol. Ctr. v Netcom On-Line Communication Servs., Inc.* (ND Cal 1995) 923 F Supp 1231; *Religious Technol. Ctr. v F.A.C.T.Net, Inc.* (D Colo 1995) 901 F Supp 1519; *Religious Technol. Ctr. v Lerma* (ED Va 1995) 897 F Supp 260.

© The Regents of the University of California

§2.36 3. Damages

On a successful misappropriation claim, CC §3426.3 allows the plaintiff to receive an injunction, lost profits, and recovery of defendant's profits for unjust enrichment. A plaintiff also may elect a to receive a reasonable royalty for the trade secret instead of damages. For a full discussion of remedies available for trade secret misappropriation, see Trade Secrets Practice in California, chap 12 (2d ed Cal CEB 1996). Reasonable royalties are usually elected and given when damages or unjust enrichment cannot be proven. Civil Code §3426.4 allows recovery of reasonable attorney fees and costs if a motion to terminate an injunction is made or resisted in bad faith or willful and malicious misappropriation is proven (or if a claim of misappropriation is made in bad faith). Willful misappropriation is determined by using "standards of subjective misconduct and objective speciousness." *Stilwell Dev., Inc. v Chen* (CD Cal 1989) 11 USPQ2d 1328. In addition, if the misappropriation is willful and malicious, the court may award exemplary damages under CC §3426.3(c).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/2 Patents and Trade Secrets/§2.37 4. Privilege and Disclosures Due to Litigation

§2.37 4. Privilege and Disclosures Due to Litigation

Lawsuits may subject trade secrets to public disclosure through discovery and public access to court proceedings. One may attempt to assert a trade secret privilege for information that may be revealed during discovery. Evidence Code §1060 states that if (a) the owner of a trade secret (or his or her agent or employee) claims this privilege, and (b) the allowance of the privilege would not conceal fraud or "otherwise work injustice," the owner of the trade secret has a privilege to refuse to disclose the secret and to prevent another person from disclosing it. In addition, to prevent a trade secret from becoming publicly available through a court proceeding, the attorney should seek a protective order (see CC §3426.5; *In re Providian Credit Card Cases* (2002) 96 CA4th 292, 116 CR2d 833; Cal Rules of Ct 2.550-2.551; Fed R Civ P 26(c)), and request the parties involved in the proceeding to enter into a nondisclosure agreement so that the information revealed during the course of litigation is not disclosed to others after litigation. See generally Trade Secrets Practice in California §§11.27-11.28 (2d ed Cal CEB 1996).

© The Regents of the University of California

§2.38 5. Economic Espionage Act of 1996

The Economic Espionage Act of 1996 (18 USC §1831-1839) was enacted to impose criminal as well as monetary penalties on individuals and organizations that misappropriate a trade secret. A trade secret is defined broadly under the Act and includes all types of information that is maintained by the owner if (a) the owner has taken reasonable steps to keep the secret, and (b) the trade secret has economic value. The Act contains two main sections, Economic Espionage and Theft of Trade Secrets. Under 18 USC §1831(a) (Economic Espionage), a person or organization is prohibited from knowingly misappropriating a trade secret with the intent or knowledge that the offense will benefit a foreign government, instrumentality, or agent. Title 18 USC §1832 (Theft of Trade Secrets) prohibits a person or organization from knowingly misappropriating a trade secret with an "intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce" for the economic benefit of someone other than the owner "and intending or knowing that the offense will injure any owner of that trade secret." Sections 1831(a) and 1832 both state that misappropriation occurs when a person or organization:

> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains [a trade secret]; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys [a trade secret]; (3) receives, buys, or possesses [a trade secret], knowing the same to have been stolen or appropriated, obtained, or converted without authorization; (4) attempts to commit any offense described in [any of] paragraphs (1) through (3); or (5) conspires with one or more other persons to commit any offense described in [any of] paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy.

A violation of the Economic Espionage section may result in a fine of up to $500,000 and/or up to 15 years of imprisonment for an individual, or a fine of up to $10,000,000 for an organization. 18 USC §1831. The penalties for violating the Theft of Trade Secrets section are a fine and/or imprisonment for up to 10 years for an individual, or a fine of up to $5,000,000 for an organization. 18 USC §1832. Note that both sections impose criminal sanctions for merely attempting or intending to misappropriate a trade secret.

In *U.S. v Yang* (6th Cir 2002) 281 F3d 534, cert denied (2003) 537 US 1170, the defendant Yang had hired as a consultant a research scientist employed by one of Yang's competitors, Avery Dennison, Inc. The consultant revealed to Yang some of Avery's trade secrets. The court found that Yang intended to obtain Avery's trade secrets from Lee, and thus violated the Economic Espionage Act of 1996. The *Yang* case demonstrates that a business should avoid any indication that it is somehow acknowledging or encouraging a consultant's use of the trade secrets of another company in connection with work done for it. If the consultant reveals the other company's trade secrets to the business, the business could be subject to criminal liability under the Act. For further discussion of the Economic Espionage Act of 1996, see Trade Secrets Practice in California §13.9A (2d ed Cal CEB 1996).

© The Regents of the University of California

3

Domain Names and Trademark Issues

I. DOMAIN NAMES
- A. Introduction §3.1
- B. Selecting Domain Name and Suffix
  - 1. Domain Name §3.2
  - 2. Suffix (Top-Level Domain Name) §3.3
- C. Due Diligence
  - 1. Domain Name as Trademark §3.4
  - 2. Where to Look? Registered and Unregistered Trademark Searches §3.5
- D. Registration of Domain Name
  - 1. Registration Procedures §3.6
  - 2. Purchasing Registered Domain Name
    - a. How to Purchase Registered Domain Name §3.7
    - b. Form: Domain Name Purchase Agreement §3.8
- E. Maintaining and Preventing Loss of Domain Name §3.9
- F. Transferring Ownership of Domain Names §3.10
- G. Infringing Domain Names
  - 1. Bringing Claim of Infringement §3.11
  - 2. Uniform Domain Name Dispute Resolution Policy (UDRP) §3.12
    - a. Elements of UDRP Claim §3.13
    - b. Selection of Arbitrators §3.14
    - c. Procedure Under UDRP §3.15
    - d. Damages and Fees §3.16
    - e. Model Form of UDRP Complaint
      - (1) Introduction §3.17
      - (2) Form: UDRP Complaint §3.18
    - f. Model Form of UDRP Response
      - (1) Introduction §3.19
      - (2) Form: UDRP Response §3.20
    - g. Appeals §3.21
  - 3. Anticybersquatting Consumer Protection Act §3.22
    - a. Elements of Cause of Action §3.23
    - b. ACPA Remedies §3.24
  - 4. Whether to Proceed Under UDRP or ACPA? §3.25

II. TRADEMARKS, SERVICE MARKS, AND TRADE NAMES
- A. Introduction §3.26
- B. Definitions of Trademarks, Service Marks, Collective Marks, Certification Marks, Trade Dress, and Trade Names §3.27
- C. Characterization of Marks §3.28
- D. Priority and Limitations to Priority §3.29
- E. Registration Procedure
  - 1. Why Federal Registration? §3.30
  - 2. Common Law and State Trademark Rights §3.31
  - 3. Unregistrable Trademarks §3.32
  - 4. Trademark Searches §3.33
  - 5. Principal and Supplemental Registers §3.34
  - 6. Intent-to-Use Applications §3.35
  - 7. Form of Application §3.36
  - 8. Application Procedure §3.37
  - 9. Contents of Application §3.38
    - a. Applicant Information §3.39
    - b. Verification §3.40
    - c. Identification and Classification of Goods and Services; Filing Fees §3.41
    - d. Bases for Filing §3.42
    - e. Drawing Requirement §3.43
    - f. Description of Mark §3.44
  - 10. Registration of Domain Names as Trademarks

a. Requirements §3.45
b. Reasons for Refusal of Registration of Domain Names §3.46
11. Trade Names §3.47
F. Madrid Protocol §3.48
G. Grant or Denial of Registration
1. Opposition, Cancellation, or Registration §3.49
2. Appeals From Denials of Registration §3.50
H. Use of Trademark Symbol §3.51
I. Duration and Renewal §3.52
J. Preservation of Trademark Rights §3.53
K. Trademark Licensing §3.54
1. Form: Trademark Guidelines §3.55
2. Form: Trademark License Agreement §3.56
L. Assignments of Trademarks
1. Generally §3.57
2. Form: Trademark Assignment §3.58
3. U.S. Patent and Trademark Office Cover Sheet (Trademarks Only) §3.59
M. Violations of Trademark Rights
1. Trademark Infringement §3.60
2. False Designation or Description §3.61
3. ACPA §3.62
4. Remedies for Trademark Infringement §3.63
5. Defenses to Trademark Infringement §3.64
6. Dilution of Famous Mark §3.65
a. Factors Bearing on Whether Mark Is Famous §3.66
b. Cybersquatting and Dilution §3.67
7. Remedies and Defenses to Anti-Dilution Claims §3.68
8. Sample Cease and Desist Letter
a. Introduction §3.69
b. Form: Sample Cease and Desist Letter §3.70

III. METATAGS AND SEARCH TERMS
A. Introduction §3.71
B. Nominative Fair Use §3.72
C. Initial Interest Confusion Test §3.73
D. Protection of Fanciful Marks §3.74
E. Misspellings of Trademarks and Direct Competitors §3.75
F. "English Words" §3.76

IV. TRADE DRESS
A. Introduction §3.77
B. Website User Interfaces §3.78
C. Trade Dress Infringement §3.79
1. Nonfunctionality
a. Overview §3.80
b. Four-Factor Test for Functionality §3.81
c. Doctrine of Aesthetic Functionality §3.82
d. Functionality and Website User Interfaces §3.83
2. Inherent Distinctiveness or Secondary Meaning
a. Inherent Distinctiveness Test §3.84
b. Product Designs and Product Packaging §3.85
c. Website User Interfaces: Product Design or Product Packaging? §3.86
3. Likelihood of Confusion in Trade Dress §3.87

© The Regents of the University of California

I. DOMAIN NAMES

§3.1 A. Introduction

Every website on the Internet is located at a specific Internet Protocol or "IP" address, which is expressed as a string of numbers indicating the location of a particular server connected to the Internet. Because numerical strings are not easy to remember, the more common way of referring to the location of an Internet site is by using a "domain name." A domain name is a string of alphanumeric characters that act as a proxy for an IP address and are expressed as "_____.com". The Domain Name System or "DNS" is a database that handles the correlation between domain names and numerical IP addresses.

A "Uniform Resource Locator" or "URL" is the unique designation of a particular file or set of files available for transfer on the Internet. A URL usually looks like this: http://www._____.com. A domain name may be used in several ways related to Internet communications, most commonly as part of a URL to be entered into an Internet browser to locate a site, or as part of an e-mail address.

Registering a domain name is an inexpensive way for a company to expand its marketing efforts. A domain name that is the same or similar to the name of a company or its products or services will increase the likelihood that consumers will be able to find the company's website. An appropriate domain name is extremely valuable because it gives businesses the opportunity to sell their products or services in geographic areas where they may not be physically located.

Because each domain name must be unique and may be used by only one registrant, disputes have arisen when different companies claim the right to use the same name. Sections 3.11-3.25 discuss how the law deals with domain name disputes. In addition, some early Internet users (known as "cybersquatters") purchased domain names that were the same or similar to the names of famous companies, hoping that the companies would buy the domain names from them at a higher price. Congress responded to this by enacting the Anticybersquatting Consumer Protection Act (ACPA), discussed in §§3.22-3.25. Sections 3.2-3.9 explain issues relating to how to select, register, and maintain a domain name, and the legal protections available for domain names.

© The Regents of the University of California

B. Selecting Domain Name and Suffix

§3.2 1. Domain Name

Most companies find it useful to have a domain name that reflects the name of the business or the services it provides so that potential customers can easily remember the name. Once a domain name is selected and registered, other domain names that are variations of the primary domain name should also be registered. These variations are called secondary domain names. Secondary domain names are typically misspellings of the primary domain name. Registering a secondary domain name is important for several reasons. First, it helps customers who do not know or cannot remember the spelling of a company's primary domain name to find the company's website. Secondary domain names also help prevent "typo-squatters" (persons who register misspelled company domain names for the purpose of reselling them) and cybersquatters (see §3.1) from registering a domain name that is similar to a company's primary domain name. A customer who inputs a secondary domain name can be forwarded automatically to the primary domain name and routed automatically to the company's website.

PRACTICE TIP: Companies should also consider registering common variants of a domain name used by operators of Internet complaint sites, such as _____sucks.com (or sux.com) or ihate_____.com. If the registrant has a prominent figure as an officer or board member, or uses a product name or mascot with a name different from the company's name, variants of those names should be registered as well. Although it is not feasible to register all possible complaint site names, especially given the creativity of those engaged in such activities, registration of the most common possibilities may make related complaint sites harder to find.

NOTE: The Truth in Domain Names Act (18 USC §2252B), enacted as §521 of the Prosecutorial Remedies and Tools Against the Exploitation of Children Today Act of 2003 (Pub L 108-21, 117 Stat 650), forbids the use of a misleading domain name with the intent to deceive a person into viewing obscenity or to deceive a minor into viewing "material that is harmful to minors" on the Internet. 18 USC §2252B(a)-(b).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.3 2. Suffix (Top-Level Domain Name)

§3.3 2. Suffix (Top-Level Domain Name)

Domain names also contain suffixes, which are the letters that follow the period after the domain name, such as .COM, .NET, and .ORG. These suffixes are referred to as "top-level domain names" (TLDs). The Internet Corporation for Assigned Names and Numbers (ICANN) has created other top-level domain names, examples of which are listed below. Note that some TLDs have restrictions on who may own them.

NOTE: In an effort to promote "more innovation, choice and change to a global Internet presently served by just 21 generic top-level domain names," ICANN has announced plans to allow applicants to design and select new top-level domain names. For more information regarding the "generic" TLD program, go to the ICANN website at http://www.icann.org/en/topics/new-gtld-program.htm.

Domain suffixes with two letters (such as .de, .mx, and .jp) have been established for over 240 countries and are referred to as "country codes." Three-letter suffixes (or "generic" TLDs) are broken down into two categories: sponsored TLDs (such as .AERO, .COOP, and .MUSEUM) and unsponsored TLDs. A sponsored TLD is associated with a particular set of stakeholders and governed by an organization that has policy-making authority for the use of the suffix. An unsponsored TLD is supervised through ICANN.

PRACTICE TIP: Although sponsorship and operation may be vested in one entity, registration of a domain name using a TLD may be made through a variety of competitive registrars.

The following are examples of TLDs along with each sponsoring or operating organization.

- .AERO is a sponsored TLD used solely by the air-transport industry and is sponsored by Société Internationale de Télécommunications Aéronautiques. http://www.information.aero.
- .BIZ is restricted for use by commercial sites and is operated by NeuLevel, Inc. http://www.neustarregistry.biz. It may only be used for a "bona fide business or commercial use."
- .BZ was originally designated as the country code for Belize, but it is now unrestricted and is often used by small businesses unable to get the name they want using the .BIZ extension. It is operated by http://www.belizenic.bz.
- .COM is probably the most common TLD and is operated by VeriSign. http://www.verisign.com/products-services/naming-and-directory-services.
- .COOP is a sponsored TLD reserved for use by cooperatives. It is sponsored by DotCooperation LLC. http://www.nic.coop.
- .EDU is reserved for postsecondary institutions accredited by an agency on the list of Nationally Recognized Accrediting Agencies maintained by U.S. Department of Education, and is registered only through Educause. http://www.educause.edu/edudomain.
- .GOV is reserved exclusively for use by the United States government. It is operated by the U.S. General Services Administration.
- .INFO is an unrestricted TLD (similar to .COM) and is operated by Afilias Ltd. http://www.afilias.info.
- .JOBS is reserved for corporate human resource managers and is sponsored by Employ Media LLC. http://www.goto.jobs. Note that this TLD cannot be used to post jobs for third parties or for general recruiting services. The TLD can be used by an employer to direct job seekers to the employment opportunities page of the employer on its own company website.
- .MIL is reserved exclusively for the United States military and is operated by the U.S. DoD Network Information Center.
- .MOBI is a "sponsored" domain reserved for consumers and providers of mobile products and services (targeting the telecommunications, media, and online industries) and its sponsor is mTLD Top Level Domain, Ltd. http://www.mtld.mobi. The rationale behind this new TLD appears to be quality assurance in the market for mobile content and services; it indicates that the content located on the applicable Internet site is optimized for

delivery to mobile devices.

- .MUSEUM is a "sponsored" domain reserved for museums. Its sponsor is the Museum Domain Management Association. http://musedoma.museum.
- .NAME is reserved for individuals and is operated by Global Name Registry. http://www.gnr.name.
- .NET is not restricted to use for any specific purpose, but is commonly used by companies involved in Internet infrastructure. It is operated by VeriSign. http://www.verisign.com/products-services/naming-and-directory-services.
- .ORG is intended for use by nonprofit organizations, but there are no formal restrictions on its use by others. It is operated by Public Interest Registry. http://www.pir.org.
- .PRO is restricted to credentialed professionals, such as physicians, lawyers, accountants, and related entities and is operated by RegistryPro. http://www.nic.pro.
- .TRAVEL is a sponsored TLD reserved for entities whose primary area of activity is the travel industry. The sponsor is Tralliance Corporation. http://www.tralliance.info.
- .TV is the country code top-level domain for the island nation of Tuvalu; however, it is unrestricted and anyone may register a .tv domain for a fee, much of the income from which goes to the government and people of Tuvalu. The TLD is often used as an abbreviation of "television" by the entertainment and media industries. The domain is operated by The .tv Corporation, a VeriSign company. http://www.tv.
- .US is a geographic extension for United States of America. It is operated by NeuStar, Inc. http://www.nic.us. Users of the US TLD must meet certain minimal nexus requirements with the United States. http://www.nic.us/policies/nexus_requirement.html.
- .WS was originally designated as the country code for Western Samoa, but is now unrestricted and is often used as an acronym for "websites." It is operated by http://www.samoanic.ws.

PRACTICE TIP: To the extent permissible under ICANN rules, consider registering a domain name with all available suffixes whenever economically feasible (for example, if registering ____.com, consider registering ____.org, ____.biz, and other available TLDs as well). In this way, the domain names are "taken off the market" so that third parties cannot use them. In addition, keep abreast of the creation of new top-level domain names on the ICANN website to register the chosen domain name with new suffixes as they become available.

For additional information on TLDs, see http://www.icann.org/tlds.

© The Regents of the University of California

C. Due Diligence

§3.4 1. Domain Name as Trademark

Before registering a domain name, counsel for an online business should perform due diligence to confirm that the domain name is not likely to infringe on a third party's trademark. See §3.3 Note. Federal trademark law generally prevents use of domain names and designations that (1) create a likelihood of confusion among consumers regarding the origin of a registered trademark owner's product or service or (2) are similar to a registered trademark. See 15 USC §1114(1). Trademark law is discussed more fully in §§3.26-3.70. As noted in §3.29, the rights of a trademark owner, including priority to use the mark, may be limited to the geographic area where the trademark is used.

© The Regents of the University of California

§3.5 2. Where to Look? Registered and Unregistered Trademark Searches

A good place to start due diligence is to look for federally registered trademarks through the database of the United States Patent and Trademark Office (USPTO), called the Trademark Electronic Search System (TESS). TESS contains all federally registered marks as well as those that are pending, expired, and abandoned. Searching TESS is free; it can be accessed through the USPTO's website at http://www.uspto.gov/main/trademarks.htm. There is a lag between the time that trademark or service mark applications are filed and the time that they are entered in the TESS database. A company should therefore check TESS several times before purchasing the desired domain name.

Because trademarks and service marks need not be federally registered to receive intellectual property protection, counsel should not limit a search to the federal level. Most states afford trademark and service mark owners common law or statutory intellectual property protection. See, *e.g.,* Bus & P C §§14200-14272. In addition, unregistered trademarks and business names can be found through search engines on the Internet. Typing the desired domain name in any search engine should yield a report of most places where the domain name is used on the Internet. Another source of information concerning unregistered trademarks and trade names is the Thomas Register, available on the Internet at http://www.thomasnet.com.

A company should also search for similar names at a large Internet product guide or e-commerce website. For example, if the desired domain name is associated with toy sales, then http://www.etoys.com should be checked because it lists many toy sellers and manufacturers by name. In addition, the Thomas Register website noted above allows the user to enter the name of a product or service, a company name, or a brand name and obtain a list of companies using that name.

Finally, counsel should consider hiring a professional trademark search firm to perform due diligence. These firms conduct searches by accessing databases of issued federal and state trademark registrations, pending federal and state registrations, and common law unregistered marks that may be found in trade name directories maintained by state secretaries of state, in buyer guides, and on the Internet.

© The Regents of the University of California

D. Registration of Domain Name

§3.6 1. Registration Procedures

The desired domain name should be registered by contracting with an issuer of domain names (otherwise known as a "registrar") that is authorized by ICANN. Using an ICANN-authorized registrar is important because such registrars are required to comply with the rules promulgated by ICANN to protect consumers. For a complete list of all ICANN-authorized registrars, visit the ICANN website at http://www.icann.org/tlds.

The first ICANN-authorized registrar was Network Solutions. Today, there are over 100 registrars, and as a result the fees for registering domain names, as well as accompanying services such as e-mail and Web hosting, have become competitive. Once a registrar is chosen, the potential purchaser should search the registrar's website to see if the desired domain name is available. The procedures for registering the desired domain name will be set forth on the registrar's website.

PRACTICE TIP: When selecting a registrar, inquire whether the registrar offers automatic renewal services to prevent an inadvertent lapse in registration. If a lapse in registration occurs, the domain name will be available for purchase by a third party.

© The Regents of the University of California

2. Purchasing Registered Domain Name

§3.7 a. How to Purchase Registered Domain Name

A domain name that is already registered may be purchased from the owner directly, or indirectly through an auction site or an online classified ad. An offer can be made to an owner directly by using the WHOIS search provided by InterNIC at http://www.internic.net/whois.html. The WHOIS search will list the owner's contact name, phone number, address, and e-mail address. An offer can also be made indirectly through an online domain name broker such as http://www.GreatDomains.com.

NOTE: Purchasing a previously registered domain name may expose a company to trademark liability if the domain name infringes another mark. To avoid potential liability for trademark infringement, searches should be conducted as discussed in §3.5 before buying a domain name that is already registered.

A form of domain name purchase agreement is in §3.8. For further discussion of procedures for transfer of ownership of domain names, and a longer form of domain name assignment agreement, see §§22.18-22.19.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.8 b. Form: Domain Name Purchase Agreement

§3.8 b. Form: Domain Name Purchase Agreement

▶ To download **Word** version, right click and choose *Save Target As*

▶ To download **WordPerfect** version, right click and choose *Save Target As*

DOMAIN NAME PURCHASE AGREEMENT

THIS DOMAIN NAME PURCHASE AGREEMENT ("Agreement") is made and entered into as of _ _[*date*]_ _ ("Effective Date") by and between _ _[*name of buyer*]_ _, a _ _[*state of incorporation*]_ _ corporation (the "Purchaser") and _ _[*name of seller*]_ _ (the "Seller").

WHEREAS, the Internet domain name _ _[*domain name*]_ _ (including all intellectual property rights and goodwill in such domain name) (the "Domain Name") is registered to Seller in the domain name registry maintained by _ _[*registrar of domain name*]_ _; and

WHEREAS, the Purchaser desires to purchase the Domain Name and Seller desires to sell the Domain Name to Purchaser.

NOW, THEREFORE, in consideration of the foregoing and of the mutual covenants and agreements contained herein, and of other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereby agree as follows:

1. PURCHASE AND SALE; CONSIDERATION. For _ _[*dollar amount*]_ _ ("Purchase Price"), Purchaser hereby purchases from Seller and Seller hereby sells to Purchaser all of Seller's right, title, and interest in and to the Domain Name (including all intellectual property rights and goodwill in such name) and in and to Seller's registration of the Domain Name with _ _[*registrar of domain name*]_ _ or any other organization entitled to register domain names ending in the ".com" top-level domain.

2. ASSIGNMENT OF DOMAIN NAME. Seller hereby assigns, remises, releases, and quitclaims to Purchaser any and all rights, title, and interest in and to the use and registration of the Domain Name, including all trademark rights, together with the goodwill of Seller's business symbolized by the Domain Name.

3. CLOSING AND ESCROW AGENT. Immediately after execution of this Agreement, Purchaser shall wire transfer _ _[*dollar amount*]_ _ to _ _[*name of escrow agent*]_ _ to hold as Escrow Agent under the Escrow Agreement among Purchaser, Seller, and Escrow Agent dated _ _[*date of escrow agreement*]_ _, and Seller shall commence transfer of the registration of the Domain Name to Purchaser in accordance with _ _[*registrar of domain name*]_ _'s domain name transfer procedures. Once this transfer is complete, Seller shall provide prompt written notice thereof to Purchaser. The Closing of the purchase and sale of the Domain Name shall occur within 5 days after Purchaser's receipt of such written notice, or such other time as agreed by the parties. At the Closing, Seller shall deliver to Purchaser documentation evidencing the completed transfer to Purchaser of the registration of the Domain Name and the Purchaser and Seller shall execute a written letter to Escrow Agent instructing Escrow Agent to release the _ _[*dollar amount held in escrow*]_ _ to Seller and any accrued interest in the escrow account to Purchaser. The balance of the Purchase Price shall be paid by Purchaser to Seller in equal installments over a period of _ _[*e.g., 12*]_ _ months from the closing date.

Comment: An escrow agent is not absolutely necessary; however, an escrow agent may facilitate the exchange of consideration and the domain name.

4. REPRESENTATIONS AND WARRANTIES. Seller represents and warrants that the transfer to Purchaser of Seller's right, title, and interest in and to the Domain Name shall be free and clear of all liens, claims, or encumbrances. Seller further represents and warrants that (a) neither Seller, nor any entity owned or controlled by Seller, owns any trademarks or copyrights in the Domain Name; (b) at the time of transferring the registration of the Domain Name to Purchaser, there shall be no fees or assessments outstanding with respect to such registration and Purchaser shall have the full right to use such registration in accordance with the rules and regulations of _ _[*registrar of domain name*]_ _ related to such registration; and (c) the Seller is not

aware that the Domain Name infringes the intellectual property rights of any third party and has received no claim of infringement from a third party.

5. PROHIBITION ON REGISTRATION OF CERTAIN DOMAIN NAMES. Seller agrees that neither Seller, nor any entity owned or controlled by Seller, shall register any Internet domain name that includes the word _ _[*second level portion of domain name*]_ _ or any domain name confusingly similar to _ _[*domain name*]_ _.

6. INDEMNIFICATION. With respect to the representations, warranties, covenants, and agreements made by each party in this Agreement, the parties shall indemnify, defend, and hold each other harmless against all liability, loss, or damage, together with all reasonable costs and expenses related thereto (including legal and accounting fees and expenses), arising from the untruth, inaccuracy, or breach of any such representations, warranties, or agreements.

Comment: If the attorney is representing the seller, this indemnification provision should be curtailed. The seller's attorney should consider limiting damages to the amount paid for the domain name.

7. ATTORNEY FEES. Purchaser shall pay all of Escrow Agent's fees and attorney fees for documents necessary to complete this Domain Name Purchase Agreement up to a maximum of _ _[*dollar amount*]_ _. Any fees in excess of this amount shall be paid one-half by each party.

8. ENTIRE AGREEMENT. This Agreement contains the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior and contemporaneous arrangements or understandings with respect thereto.

9. COUNTERPARTS. This Agreement may be executed in any number of counterparts, and each such counterpart hereof shall be deemed to be an original instrument, but all such counterparts together shall constitute but one agreement.

10. GOVERNING LAW. This Agreement shall be governed by and construed in accordance with the laws of the State of California without regard to its conflict of laws rules.

IN WITNESS WHEREOF, the undersigned have duly executed this Agreement, or have caused this Agreement to be duly executed on their behalf, as of the Effective Date.

Date: _ _ _ _ _ _

_ _[*NAME OF BUYER*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name of buyer*]_ _
Its: _ _[*Title*]_ _
_ _[*Buyer's address*]_ _

Date: _ _ _ _ _ _

_ _[*NAME OF SELLER*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name of seller*]_ _
Its: _ _[*Title*]_ _
_ _[*Seller's address*]_ _

© The Regents of the University of California

§3.9 E. Maintaining and Preventing Loss of Domain Name

Due diligence should continue to be performed after the domain name is registered to prevent loss of the domain name. There are many ways a domain name owner can lose a domain name. For example, a domain name may be lost if the registrar considers it abandoned, which usually occurs if the owner fails to pay the renewal fees for the domain name. Loss of the domain name can also occur if the contact information given to the registrar is not updated or the name of an employee who has left the business is listed as the contact person. If the registrar causes loss of a domain name, the owner may file a complaint with ICANN, placing ICANN on notice of the registrar's actions. A complaint may also be submitted to the California Department of Consumer Affairs at http://www.dca.ca.gov. In November 2004, ICANN implemented a new domain name transfer policy intended to standardize selection and registration processes and strengthen protection against unauthorized transfers. See the policy at http://www.icann.org/transfers.

In *Kremen v Cohen* (9th Cir 2003) 337 F3d 1024, a domain name registrar transferred a registered domain name to a con man based on a forged letter. Plaintiff Kremen obtained rights to the domain name "sex.com" from Network Solutions, a domain name registrar, on behalf of his company, Online Classified. Defendant Cohen sent Network Solutions a fraudulent letter claiming that Kremen had been dismissed and requesting transfer of the domain name to himself. Network Solutions made no attempt to contact Kremen or confirm the statements made in the letter and transferred the domain name to Cohen. Kremen (unable to pursue Cohen, who had been declared a fugitive from justice by a federal district judge) sued Network Solutions for conversion of property, among other claims. The lower court rejected Kremen's claim of conversion, finding that the domain name was intangible property to which the tort of conversion did not apply. The Ninth Circuit Court of Appeals held that, although the right to use a domain name is an intangible personal property right, it is nonetheless protected by California conversion law and that Network Solutions was liable for carelessly giving away Kremen's domain name. 337 F3d at 1035.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.10 F. Transferring Ownership of Domain Names

§3.10 F. Transferring Ownership of Domain Names

Procedures for purchasing domain names, including a form of domain name purchase agreement, are discussed in §3.7-3.8. For further discussion of the procedures for changing the ownership of a domain name and a longer form of assignment of a domain name, see §§22.18-22.19.

© The Regents of the University of California

G. Infringing Domain Names

§3.11 1. Bringing Claim of Infringement

A claim against an infringing domain name may be brought under the Uniform Domain Name Dispute Resolution Policy (UDRP) of ICANN or the Anticybersquatting Consumer Protection Act (ACPA) (15 USC §1125(d)) if the defendant's domain name is infringing on a trademark. The procedures and requirements for bringing an action under the UDRP and ACPA are discussed in §§3.12-3.24. For discussion of the factors to consider in deciding whether to pursue a claim under the UDRP or under the ACPA, see §3.25.

© The Regents of the University of California

§3.12 2. Uniform Domain Name Dispute Resolution Policy (UDRP)

A claim under the UDRP initiates a binding arbitration proceeding that is administered by an ICANN-authorized arbitrator. The arbitration proceeding is largely governed by the Rules for Uniform Domain Name Dispute Resolution Policy (UDRP Rules), which can be found at http://www.icann.org/dndr/udrp/uniform-rules.htm. ICANN coordinates and manages the Internet's Domain Name System (DNS), the allocation of IP address space, the assignment of protocol parameters, and the management of the root server system. Domain name owners are required to consent to UDRP's authority when registering a domain name with an ICANN-authorized registrar. A dispute may be brought under the UDRP if it concerns a domain name that is infringing another's mark.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.13 a. Elements of UDRP Claim

§3.13 a. Elements of UDRP Claim

To bring a successful complaint under the UDRP, the following must be asserted and proven (UDRP ¶4(a)):

- The domain name in dispute is identical or confusingly similar to a trademark or service mark in which the complainant has rights;
- The owner of the domain name in dispute has no rights or legitimate interests in the domain name; and
- The domain name in dispute is considered to be registered and is being used in bad faith.

Under UDRP ¶4(c), an owner of a domain name can refute the assertion that the owner has no rights or a legitimate interest in the domain name if one of the following are shown:

- Before notice of the dispute, the owner used or was preparing to use the domain name or a name corresponding to the domain name in connection with a commercial purpose;
- The domain name owner is commonly known or identified by the domain name even though the domain name is not a registered trademark or service mark; or
- The domain name owner uses the domain name for a legitimate noncommercial purpose or makes fair use of the domain name and there is no intent to mislead consumers or to tarnish the trademark or service mark.

UDRP ¶4(b) also sets forth a list of factors used to determine whether the domain name owner is using the name in bad faith. The factors are as follows:

- Circumstances showing that the domain name owner acquired the domain name primarily to sell it to the owner of the trademark or service mark or to a competitor for an amount greater than the acquirer paid for it;
- The domain name owner registered the domain name to prevent the trademark or service mark owner from registering the domain name, and the domain name owner has engaged in a pattern of this conduct;
- The domain name was registered primarily to disrupt the business of the competitor; or
- The domain name owner intentionally used the domain name to attract Internet users to the owner's website, for commercial gain, by creating a likelihood of confusion with the trademark or service mark.

For discussion of the application of UDRP to Internet "gripe" sites, such as the infamous "sucks.com" websites, see §20.29.

© The Regents of the University of California

§3.14 b. Selection of Arbitrators

Complainants may choose an arbitrator from several approved ICANN arbitration providers, including the Asian Domain Name Dispute Resolution Center, CPR Institute for Dispute Resolution, the National Arbitration Forum, and the World Intellectual Property Organization. An updated list of all ICANN-authorized arbitration providers can be found on the ICANN website, http://www.icann.org. Each of these arbitration providers offers information on the procedures required to bring a claim under the UDRP. In addition, a form complaint and response can usually be found on the arbitration provider's website.

© The Regents of the University of California

§3.15 c. Procedure Under UDRP

Filing a complaint with the selected arbitration provider begins the arbitration process. UDRP Rules ¶3. Once a complaint is filed, the party against whom the complaint is made must file a response. UDRP Rules ¶5. An administrative panel appointed by the arbitration provider typically issues a decision within 17 days after the appointment of the panel. UDRP Rules ¶15. The entire process, however, takes approximately 50 days. After receiving the panel's decision, the arbitration provider will notify the concerned registrar of the decision to effectuate the ruling of the arbitration panel. UDRP Rules ¶16. See generally UDRP Rules at http://www.icann.org/dndr/udrp/uniform-rules.htm.

© The Regents of the University of California

§3.16 d. Damages and Fees

An administrative panel cannot issue a monetary award, but UDRP Rules ¶3 authorizes the panel to cancel, transfer, or make changes to the infringing domain name. Although the remedies provided under the UDRP are minimal, the arbitration proceeding is less expensive than a lawsuit commenced in court. A complaint that involves a dispute concerning one to five domain names and a single panelist costs approximately $1500. For a three-person panel, the cost is approximately $3000.

© The Regents of the University of California

e. Model Form of UDRP Complaint

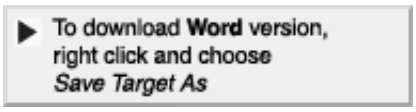
§3.17 (1) Introduction

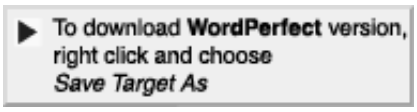
In §3.18 is a model form of complaint under the UDRP with instructions from the World Intellectual Property Organization. See generally http://www.wipo.int/amc/en/domains/index.html.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.18 (2) Form: UDRP Complaint

§3.18 (2) Form: UDRP Complaint





Before the:

WORLD INTELLECTUAL PROPERTY ORGANIZATION
ARBITRATION AND MEDIATION CENTER

_ _[*NAME AND ADDRESS OF COMPLAINANT*]_ _, **(Complainant)**	)	**Disputed Domain Name(s):** _ _[*The contested domain name(s)*]_ _
vs	)	
_ _[*NAME AND ADDRESS OF RESPONDENT*]_ _, **(Respondent)**	)	

COMPLAINT
(UDRP Rules ¶3(b))

I. INTRODUCTION

[1.] This Complaint is hereby submitted for decision in accordance with the Uniform Domain Name Dispute Resolution Policy (UDRP), approved by the Internet Corporation for Assigned Names and Numbers (ICANN) on October 24, 1999, the Rules for Uniform Domain Name Dispute Resolution Policy (the UDRP Rules), approved by ICANN on October 24, 1999, and the WIPO Supplemental Rules for Uniform Domain Name Dispute Resolution Policy (the UDRP Supp Rules).

II. THE PARTIES
A. The Complainant
(UDRP Rules ¶3(b)(ii)-(iii))

[2.] The Complainant in this administrative proceeding is _ _[*provide full name and, if relevant, legal status, place of incorporation, and principal place of business*]_ _**.**

[3.] The Complainant's contact details are:

_ _[*Address*]_ _
_ _[*Telephone*]_ _
_ _[*Fax*]_ _
_ _[*E-mail*]_ _

[4.] The Complainant's authorized representative in this administrative proceeding is: _ _[*name; provide contact information as well*]_ _**.**

[5.] The Complainant's preferred method of communications directed to the Complainant in this administrative proceeding is:

Electronic-only material:

Method: **E-mail**

Address: [*Specify one e-mail address*]

Contact: [*Identify name of one contact person*]

Material including hardcopy:

Method: [*Specify one: fax, post/courier*]

Address: [*Specify one address, if applicable*]

Fax: [*Specify one fax number*]

Contact: [*Identify name of one contact person*]

B. The Respondent
(UDRP Rules ¶3(b)(v))

[6.] According to _ _[*indicate why the person/entity identified in the Complaint has been identified as the Respondent, e.g., the concerned registrar's Whois database.*]**_ _, the Respondent in this administrative proceeding is _ _**[*identify Respondent (the domain name holder), including full name, and if relevant, legal status, place of incorporation and principal place of business, or residence)*]**_ _. Copies of the printout of the database search(es) conducted on _ _**[*date*]**_ _ are provided as Annex _ _**[*Annex number*]**_ _.**

[7.] All information known to the Complainant regarding how to contact the Respondent is as follows:

[*Provide all contact details (postal address, telephone number, fax number, e-mail addresses) for the respondent, including those that may have been used successfully in the course of pre-complaint dealings and those available from any Whois look-up service.*]

[*If there is more than one Respondent, provide the contact details for each Respondent and describe the relationship between them, which justifies them being named in a common complaint.*]

III. THE DOMAIN NAME(S) AND REGISTRAR(S)
(UDRP Rules ¶3(b)(vi)-(vii))

[8.] This dispute concerns the domain name(s) identified below:

[*Identify precisely the domain name(s) in issue.*]

[9.] The registrar(s) with which the domain name(s) _ _[*is/are*]**_ _ registered _ _**[*is/are*]**_ _:**

[*Provide the name and full contact details of the registrar(s) with which the domain name(s) (is/are) registered.*]

IV. JURISDICTIONAL BASIS FOR THE ADMINISTRATIVE PROCEEDING
(UDRP Rules ¶¶3(a), 3(b)(xv))

[10.] This dispute is properly within the scope of the Policy and the Administrative Panel has jurisdiction to decide the dispute. The registration agreement, pursuant to which the domain name(s) that _ _[*is/are*]**_ _ the subject of this Complaint _ _**[*is/are*]**_ _ registered, incorporates the Policy. _ _**[*If relevant, indicate when the domain name(s) (was/were) registered and specify the provision of the registration agreement that makes the Policy applicable to the domain names(s).*]**_ _ A true and correct copy of the domain name dispute policy that applies to the domain name(s) in question is provided as Annex _ _**[*Annex number*]**_ _ to this Complaint.**

V. FACTUAL AND LEGAL GROUNDS
(UDRP ¶¶4(a), (b), (c); UDRP Rules ¶3)

[*In completing this Section V., do not exceed the 5000-word limit: UDRP Supp Rules ¶10(a). Relevant documentation in support of the Complaint should be submitted as Annexes, with a schedule indexing such Annexes. Copies of case precedents or commentaries that are referred to for support should be referred to with complete citations and, if not voluminous, submitted as Annexes.*]

[11.] This Complaint is based on the following grounds:

(a) The domain name(s) _ _[*is/are*]**_ _ identical or confusingly similar to a trademark or service mark in which**

the Complainant has rights;

(UDRP ¶4(a)(i); UDRP Rules ¶¶3(b)(viii), (b)(ix)(1))

[*In accordance with UDRP Rules ¶3(b)(viii), specify the trademark(s) or service mark(s) on which the Complaint is based and, for each mark, describe the goods or services, if any, in connection with which the mark is used. A separate description may also be given of the goods or services with which the Complainant intends to use the mark in the future. If applicable, attach copies of the registration certificates for the relevant marks.*]

[*In accordance with UDRP Rules ¶3(b)(ix)(1), describe the manner in which the domain name(s) (is/are) identical or confusingly similar to a trademark or service mark in which the Complainant has rights.*]

(b) The Respondent has no rights or legitimate interests in respect of the domain name(s);

(UDRP ¶4(a)(i); UDRP Rules ¶3(b)(ix)(2))

[*In accordance with UDRP Rules ¶3(b)(ix)(2), describe why the Respondent should be considered as having no rights or legitimate interests in respect of the domain name(s) that (is/are) the subject of the Complaint. Attention should be paid to any relevant aspects of the UDRP ¶4(c), including:*

Whether before any notice to the Respondent of the dispute, there is any evidence of the Respondent's use of, or demonstrable preparations to use, the domain name(s) or a name corresponding to the domain name(s) in connection with a bona fide offering of goods or services;

Whether the Respondent (as an individual, business, or other organization) has been commonly known by the domain name, even if the Respondent has acquired no trademark or service mark rights;

Whether the Respondent is making a legitimate non-commercial or fair use of the domain name(s), without intent for commercial gain misleadingly to divert consumers or to tarnish the trademark or service mark at issue.]

(c) The domain name(s) _ _[*was/were*]_ _ registered and _ _[*is/are*]_ _ being used in bad faith.

(UDRP ¶4(a)(iii), 4(b); UDRP Rules ¶3(b)(ix)(3))

[*In accordance with UDRP Rules ¶3(b)(ix)(3), describe why the domain name(s) should be considered as having been registered and used in bad faith by the Respondent. Attention should be paid to any relevant aspects of UDRP Rules ¶4(b), including:*

Circumstances indicating that the domain name(s) (was/were) registered or acquired primarily for the purpose of selling, renting, or otherwise transferring the domain name registration(s) to the owner of the trademark or service mark (normally the Complainant) or to a competitor of that Complainant, for valuable consideration in excess of the Respondent's out-of-pocket costs directly related to the domain name(s); or

Whether the domain name(s) (was/were) registered in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that the Respondent has engaged in a pattern of such conduct; or

Whether the domain name(s) (was/were) registered primarily for the purpose of disrupting the business of a competitor; or

Whether by using the domain name(s), the Respondent intentionally attempted to attract, for commercial gain, Internet users to the Respondent's website or other on-line location, by creating a likelihood of confusion with the Complainant's mark as to the source, sponsorship, affiliation, or endorsement of the Respondent's website or location or of a product or service on the Respondent's website or location.]

VI. REMEDIES REQUESTED
(UDRP Rules ¶3(b)(x))

[12.] In accordance with UDRP ¶4(i), for the reasons described in Section V above, the Complainant requests

the Administrative Panel appointed in this administrative proceeding _ _[*choose one per domain name: "issue a decision that the contested domain name(s) be transferred to the Complainant"/"be cancelled"*]**_ _.**

VII. ADMINISTRATIVE PANEL
(UDRP Rules ¶3(b)(iv))

[13.] The Complainant elects to have the dispute decided by a _ _[*choose one: "single-member Administrative Panel"/"three-member Administrative Panel"*]**_ _.**

[*If a three-member Administrative Panel is designated, the names of three persons must be provided, one of whom the Center shall attempt to appoint to the Administrative Panel in accordance with UDRP Rules ¶6 and UDRP Supp Rules ¶7. The names of the nominees may be taken from the Center's published list of panelists at http://arbiter.wipo.int/domains/panel/panelists.html, or that of any other ICANN-accredited dispute resolution service provider.*]

VIII. MUTUAL JURISDICTION
(UDRP Rules ¶3(b)(xiii))

[14.] In accordance with UDRP Rules ¶3(b)(xiii) of the Rules, the Complainant will submit, with respect to any challenges that may be made by the Respondent to a decision by the Administrative Panel to transfer or cancel the domain name(s) that _ _[*is/are*]**_ _ the subject of this Complaint, to the jurisdiction of the courts at**

[*Add one of the following alternatives*]

[*Alternative 1*]

the location of the principal office of the concerned registrar.

[*Alternative 2*]

the location of the domain name holder's address, as shown for the registration of the domain name(s) in the concerned registrar's Whois database at the time of the submission of the Complaint to the Center.

[*Alternative 3*]

the location of the principal office of the concerned registrar and the domain name holder's address, as shown for the registration of the domain name(s) in the concerned registrar's Whois database at the time of the submission of the Complaint to the Center.

[*Continue*]

[*A Mutual Jurisdiction election must be made for each domain name that is the subject of the Complaint.*]

IX. OTHER LEGAL PROCEEDINGS
(UDRP Rules ¶3(b)(xi))

[15.] [*If any, identify other legal proceedings that have been commenced or terminated in connection with or relating to the domain name(s) that (is/are) the subject of the Complaint and summarize the issues that are the subject of (that/those) proceeding(s).*]

X. COMMUNICATIONS
(UDRP Rules ¶¶2(b), 3(b)(xii); UDRP Supp Rules ¶¶3-4)

[16.] A copy of this Complaint, together with the cover sheet as prescribed by the Supplemental Rules, has been sent or transmitted to the Respondent on _ _[*date*]**_ _ by _ _**[*indicate method(s) of communication and contact details used, with reference to UDRP Rules ¶2(b)*]**_ _.**

[17.] A copy of this Complaint, has been sent or transmitted to the concerned registrar(s) on _ _[*date*]**_ _ by _ _**[*indicate method(s) of communication and contact details used*]**_ _.**

[18.] This Complaint is submitted to the Center in electronic form (except to the extent not available for annexes), and in 4 sets together with the original.

XI. PAYMENT
(UDRP Rules ¶19; UDRP Supp Rules, Annex D)

[19.] As required by the UDRP Rules and UDRP Supp Rules, payment in the amount of _ _[*dollar amount*]_ _ has been made by _ _[*specify method*]_ _.

XII. CERTIFICATION
(UDRP Rules ¶3(b)(xiv))

[20.] The Complainant agrees that its claims and remedies concerning the registration of the domain name(s), the dispute, or the dispute's resolution shall be solely against the domain name holder and waives all such claims and remedies against (a) the WIPO Arbitration and Mediation Center and Panelists, except in the case of deliberate wrongdoing, (b) the concerned registrar(s), (c) the registry administrator, (d) the Internet Corporation for Assigned Names and Numbers, as well as their directors, officers, employees, and agents.

[21.] The Complainant certifies that the information contained in this Complaint is to the best of the Complainant's knowledge complete and accurate, that this Complaint is not being presented for any improper purpose, such as to harass, and that the assertions in this Complaint are warranted under the Rules and under applicable law, as it now exists or as it may be extended by a good-faith and reasonable argument.

Respectfully submitted,

Date: _ _ _ _ _ _ __[*Signature*]__
_ _[*Typed name*]_ _

© The Regents of the University of California

f. Model Form of UDRP Response

§3.19 (1) Introduction

In §3.20 is a model form of response under the UDRP with instructions from the World Intellectual Property Organization. See generally http://arbiter.wipo.int/domains/guide.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.20 (2) Form: UDRP Response

§3.20 (2) Form: UDRP Response

▶ To download **Word** version, right click and choose *Save Target As*

▶ To download **WordPerfect** version, right click and choose *Save Target As*

Before the:

WORLD INTELLECTUAL PROPERTY ORGANIZATION
ARBITRATION AND MEDIATION CENTER

_ _[*NAME AND ADDRESS OF COMPLAINANT AS STATED IN COMPLAINT*]_ _, **(Complainant)**	**No.** _ _[*Indicate case number*]_ _
vs	_ _[*Contested domain name(s)*]_ _
_ _[*NAME AND ADDRESS OF RESPONDENT*]_ _, **(Respondent)**	

RESPONSE
(UDRP Rules ¶5(b))

I. INTRODUCTION

[1.] On _ _[*indicate date on which the Notification of Complaint and Commencement of Administrative Proceeding was received*]_ _**, the Respondent received a Notification of Complaint and Commencement of Administrative Proceeding from the WIPO Arbitration and Mediation Center (the Center) by** _ _[*e-mail/fax/post/courier*]_ _ **informing the Respondent that an administrative proceeding had been commenced by the Complainant in accordance with the Uniform Domain Name Dispute Resolution Policy (UDRP), approved by the Internet Corporation for Assigned Names and Numbers (ICANN) on October 24, 1999, the Rules for Uniform Domain Name Dispute Resolution Policy (the UDRP Rules), approved by ICANN on October 24, 1999, and the WIPO Supplemental Rules for Uniform Domain Name Dispute Resolution Policy (the UDRP Supp Rules). The Center set** _ _[*insert date*]_ _ **as the last day for the submission of a Response by the Respondent.**

II. RESPONDENT'S CONTACT DETAILS
(UDRP Rules ¶5(b)(ii)-(iii))

[2.] The Respondent's contact details are: _ _[*name, address, telephone, fax, e-mail*]_ _**.**

[*If there is more than one Respondent, provide the above information for each.*]

[3.] The Respondent's authorized representative in this administrative proceeding is:

[*If relevant, identify authorized representative and provide all contact details, including postal address, telephone number, fax number, e-mail address; if there is more than one authorized representative, provide contact details for each.*]

[4.] The Respondent's preferred method of communications directed to the Respondent in this administrative proceeding is:

Electronic-only material:

Method:	**E-mail**
Address:	[*Specify one e-mail address*]
Contact:	[*Identify name of one contact person*]

Material including hardcopy:

Method:	[*Specify one: fax, post/courier*]
Address:	[*Specify one address, if applicable*]
Fax:	[*Specify one fax number*]
Contact:	[*Identify name of one contact person*]

III. RESPONSE TO STATEMENTS AND ALLEGATIONS MADE IN COMPLAINT (UDRP ¶4(a), (b), (c); UDRP Rules ¶5)

[*In completing this Section III., do not exceed the 5000-word limit: UDRP Supp Rules ¶10(b). Relevant documentation in support of the Response should be submitted as Annexes, with a schedule indexing such documents. Case precedents or commentaries that are referred to for support should be referred to with complete citations and, if not voluminous, submitted as Annexes.*]

[5.] The Respondent hereby responds to the statements and allegations in the Complaint and respectfully requests the Administrative Panel to deny the remedies requested by the Complainant.

[*UDRP Rules ¶5(b)(i) instruct the Respondent in its Response to "Respond specifically to the statements and allegations contained in the complaint and include any and all bases for the Respondent (domain name holder) to retain registration and use of the disputed domain name." For a complainant to succeed, it must establish that each of the three conditions under UDRP ¶¶4(a)(i), (ii), (iii) are satisfied. With reference to that ¶4(a), in this section the Respondent may wish to discuss some or all of the following, to the extent relevant and supported by evidence:*]

A. Whether the domain name(s) _ _[*is/are*]_ _ identical or confusingly similar to a trademark or service mark in which the Complainant has rights;

(UDRP ¶4(a)(i))

[*In this connection, consideration may, for example, be given to the following:*]

[*Any challenges to the trade or service mark rights asserted by the Complainant.*]

[*A refutation of the arguments made by the Complainant concerning the manner in which the domain name(s) (is/are) allegedly identical or confusingly similar to a trademark or service mark in which the Complainant claims it has rights.*]

B. Whether the Respondent has rights or legitimate interests in respect of the domain name(s);

(UDRP ¶4(a)(ii))

[*In this connection, consideration may, for example, be given to the following:*]

[*A refutation of the arguments made by the Complainant as to why the Respondent should be considered as having no rights or legitimate interests in respect of the domain name(s) that (is/are) the subject of the Complaint. Evidence should be submitted in support of any claims made by the Respondent concerning its alleged rights or legitimate interests in the domain name(s).*]

[*UDRP ¶4(c) sets out examples of circumstances demonstrating the Respondent's rights to or legitimate interests in the domain name(s) for the purposes of UDRP ¶4(a)(ii). With reference to that ¶4(c), to the extent argued by the Complainant, the Respondent should discuss and show that:*

Before the Respondent received any notice of the dispute, there is evidence of the Respondent's use of, or demonstrable preparations to use, the domain name(s) or a name corresponding to the domain name(s) in connection with a bona fide offering of goods or services;

The Respondent (as an individual, business, or other organization) has been or is commonly known by the domain name(s) in issue, even if the Respondent has acquired no trademark or service mark rights;

The Respondent is making a legitimate non-commercial or fair use of the domain name(s), without intent for commercial gain misleadingly to divert consumers or to tarnish the trademark(s) or service mark(s) a issue.]

C. Whether the domain name(s) _ _[*has/have*]**_ _ been registered and _ _**[*is/are*]**_ _ being used in bad faith.**

(UDRP ¶4(a)(iii))

[*In this connection, consideration may, for example, be given to the following:*]

[A refutation of the arguments made by the Complainant as to why the domain name(s) should be considered as registered and used in bad faith.]

[*UDRP ¶4(b) identifies several examples of circumstances that an Administrative Panel could consider as constituting bad faith. With reference to that ¶4(b), to the extent argued by the Complainant, the Respondent should discuss and show that:*

The domain name(s) (was/were) not registered or acquired primarily for the purpose of selling, renting, or otherwise transferring the domain name registration(s) to the Complainant, as the alleged owner of the trademark or service mark, or to a competitor of the Complainant, for valuable consideration in excess of the Respondent's out-of-pocket costs directly related to the domain name(s);

The domain name(s) (was/were) not registered in order to prevent the Complainant from reflecting the mark in a corresponding domain name and, in connection therewith, the Respondent has not engaged in a pattern of such conduct;

The Complainant and the Respondent are not competitors and/or the domain name(s) (was/were) not registered by the Respondent primarily to disrupt the Complainant's business; and

The domain name(s) (was/were) not registered by the Respondent in an intentional attempt to attract for commercial gain Internet users to the Respondent's Website or other on-line location by creating a likelihood of confusion with the Complainant's mark as to the source, sponsorship, affiliation, or endorsement of the Respondent's Website or location or of a product or service on the Respondent's Website or location.]

[D.] If appropriate and the allegation can be substantiated with evidence, the Rules provide that a Respondent may ask the Panel to make a finding of reverse domain name hijacking (UDRP Rules ¶15(e)).

IV. ADMINISTRATIVE PANEL
(UDRP Rules ¶¶5(b)(iv)-(v), 6; UDRP Supp Rules ¶7)

[6.] The Respondent elects to have the dispute decided by a _ _[*state "single-member Administrative Panel" if the Complainant has asked for a single-member Administrative Panel and the Respondent agrees with that election. If the Respondent does not agree and wants a three-member Administrative Panel instead, state "three-member Administrative Panel." Note that in the latter case the Respondent must pay half of the Center's fee for a three-member Administrative Panel, as set out in Supplemental Rules, Annex D. If the Complainant has indicated it wants a three-member Administrative Panel, then the Respondent does not have the option of choosing a single-member Administrative Panel*]**_ _.**

[*If the Respondent designates a three-member Administrative Panel, or if the Complainant has designated a three-member Panel, the Respondent must provide the names of three persons, one of whom the Center will endeavor to appoint to the Administrative Panel in accordance with UDRP Rules ¶6 and UDRP Supp Rules ¶7. The names of these three nominees may be taken from the Center's published list of panelists at*

http://arbiter.wipo.int/domains/panel/panelists.html, or that of any other ICANN-accredited dispute resolution service provider.]

V. OTHER LEGAL PROCEEDINGS
(UDRP Rules ¶5(b)(vi))

[7.] _ _[*If any, identify other legal proceedings that have been commenced or terminated in connection with or relating to the domain name(s) that (is/are) the subject of the Complaint and summarize the issues that are the subject of (that/those) proceeding(s)*]_ _

VI. COMMUNICATIONS
(UDRP Rules ¶¶2(b), 5(b)(vii); UDRP Supp Rules ¶3)

[8.] A copy of this Response has been sent or transmitted to the Complainant on _ _[*date*]_ _ **by** _ _[*indicate methods of communication and contact details used, with reference to UDRP Rules ¶2(b)*]_ _**.**

[9.] This Response is submitted to the Center in electronic form (except to the extent not available for annexes), and in four (4) sets together with the original.

VII. PAYMENT
(UDRP Rules ¶5(c); UDRP Supp Rules, Annex D)

[10.] _ _[*If relevant, state: "In view of the Complainant's designation of a single-member Panel and the Respondent's designation of a three-member Panel, the Respondent hereby submits payment in the amount of USD (amount) by (method)".*]_ _

VIII. CERTIFICATION
(UDRP Rules ¶5(b)(viii); UDRP Supp Rules ¶12)

[11.] The Respondent agrees that, except in respect of deliberate wrongdoing, an Administrative Panel, the World Intellectual Property Organization, and the Center shall not be liable for any act or omission in connection with the administrative proceeding.

[12.] The Respondent certifies that the information contained in this Response is to the best of the Respondent's knowledge complete and accurate, that this Response is not being presented for any improper purpose, such as to harass, and that the assertions in this Response are warranted under the Rules and under applicable law, as it now exists or as it may be extended by a good-faith and reasonable argument.

Respectfully submitted,

Date: _ _ _ _ _ _ __[*Signature*]__
_ _[*Typed name*]_ _

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.21 g. Appeals

§3.21 g. Appeals

The decision of the arbitration panel may be appealed in court. UDRP ¶4(k). Because the registrar must implement the panel's decision within 10 days after receiving it, the appeal should be filed before the 10-day period expires. UDRP ¶4(k).

© The Regents of the University of California

§3.22 3. Anticybersquatting Consumer Protection Act

Before the enactment in 1999 of the Anticybersquatting Consumer Protection Act (ACPA) (15 USC §1125(d)), mark owners used the Federal Trademark Dilution Act of 1995, codified in 15 USC §1125(c) (sometimes called the "Anti-Dilution Act"), to assert claims against domain name infringers such as cybersquatters. Believing that the Anti-Dilution Act did not provide adequate protection to domain name owners, Congress implemented the ACPA to bridge the gaps in the Anti-Dilution Act.

An action under the ACPA may be brought against an infringer based on causes of action such as trademark infringement, dilution, or bad faith, or against domain names through in rem jurisdiction. See *Harrods Ltd. v Sixty Internet Domain Names* (4th Cir 2002) 302 F3d 214. ACPA provides that a trademark holder may proceed in rem when the trademark holder either cannot obtain in personam jurisdiction over "a person who would have been a defendant" or is unable through exercising due diligence to find a person who would be a defendant. 15 USC §1125(d)(2)(A)(ii).

Under the ACPA, an exercise of due diligence requires the following (15 USC §1125(d)(2)(A)(ii)(II)):

> (aa) sending a notice of the alleged violation and intent to proceed under this paragraph to the registrant of the domain name at the postal and e-mail address provided by the registrant to the registrar; and
> (bb) publishing notice of the action as the court *may direct* promptly after filing the action. [Emphasis added.]

In *Yahoo!, Inc. v Yahooahtos.com* (ED Va, Aug. 8, 2006, No. 1:05cv1441) 2006 US Dist Lexis 54902, the federal district court held that "may direct" should not be interpreted to make publication mandatory, and that where domain name registrants have received actual notice in the manner prescribed by 15 USC 1125(d)(2)(A)(ii)(II)(aa), any further notice by publication would be superfluous.

The ACPA applies retroactively to all domain names, regardless of when the domain name was registered; however, a complainant may seek damages only for domain names registered after November 2, 1999. *Mattel, Inc. v Internet Dimension, Inc.* (SD NY, July 13, 2000, No. 99 CIV 10066) 2000 US Dist Lexis 9747.

Several important cases have been decided under the ACPA, including *Shields v Zuccarini* (3rd Cir 2001) 254 F3d 476. In *Shields,* the U.S. Court of Appeals for the Third Circuit held that registering domain names that are intentional misspellings of a distinctive or famous name violates the ACPA. The court awarded the plaintiff damages under the ACPA as well as attorney fees, finding that the infringer's actions were egregious and in bad faith.

NOTE: There are separate federal and state cyberpiracy statutes applicable to the use of domain names that are the same or similar to the names of individuals. Title 15 USC §1129(a)(1)(A) creates civil liability for anyone who registers a domain name that is the same or "substantially and confusingly similar" to the name of another living person without that person's consent, with specific intent to profit by selling the name to that person or a third party. California has its own version of this statute (see Bus & P C §§17525-17528), but the California law also applies to the names of deceased persons and eliminates the federal requirement of a specific intent to profit from selling the domain name (see §3.23). The California statute does require a showing of a bad faith intent to register, traffic in, or use an individual's name. See Bus & P C §17525.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.23 a. Elements of Cause of Action

§3.23 a. Elements of Cause of Action

To prove a cause of action for damages under the ACPA (15 USC §1125(d)(1)(A)):

- The domain name must be:
- Identical or confusingly similar to a mark that was distinctive when the domain name was registered; or
- Identical, confusingly similar to, or dilutive of a mark that was famous when the domain name was registered; and
- The defendant must register, traffic in, or use the domain name with a bad faith intent to profit.

Nine nonexclusive factors are used in determining whether the defendant has a bad faith intent (15 USC §1125(d)(1)(B)):

- The trademark or other intellectual property rights of the defendant in the domain name;
- The extent to which the domain name consists of the legal name of the defendant or a name that is otherwise commonly used to identify that person;
- The defendant's prior use of the domain name in connection with a bona fide offering of any goods or services;
- The defendant's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;
- The defendant's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;
- The defendant's offer to transfer, sell, or assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name for a bona fide offering of any goods or services;
- Providing material and misleading false contact information when applying for the registration of the domain name, intentionally failing to maintain accurate contact information, or prior conduct indicating a pattern of such conduct;
- The defendant's registration or acquisition of multiple domain names that the person knows are identical or confusingly similar to marks that are distinctive of such domain names at the time of registration, without regard to the goods or services of the parties; and
- The extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of 15 USC §1125(c)(1).

See *Lahoti v VeriCheck, Inc*. (9th Cir 2009) 586 F3d 1190. A fact-specific inquiry is necessary to establish the "bad faith" element of a violation under the ACPA. *Interstellar Starship Servs., Ltd. v EPIX, Inc.* (9th Cir 2002) 304 F3d 936, 946. A plaintiff's reasonable belief that use of the allegedly infringing domain name was lawful precludes a finding of bad faith under 15 USC §1125(d)(1)(B), the ACPA's safe harbor provision. 304 F3d at 946. See also *Healix Infusion Therapy, Inc. v Murphy* (SD Tex, Sept. 2, 2008, No. H-08-0337) 2008 US Dist Lexis 67723 (requisite bad faith to support cybersquatting claim not present when defendant did not know plaintiff used domain name "confusingly similar" to name he sought to register).

The ACPA includes a "safe harbor" for domain registrants who "believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful." 15 USC §1125(d)(1)(B)(ii). Courts have interpreted this safe harbor narrowly. In *Virtual Works, Inc. v Volkswagen of Am., Inc.* (4th Cir 2001) 238 F3d 264, the court held that a domain registrant who acts partially in bad faith is not entitled to the safe harbor. In *Audi AG v D'Amato* (6th Cir 2006) 469 F3d 534, 549, the court stated that the safe harbor is available "only in the most unusual cases."

In *Lahoti v VeriCheck, Inc., supra,* the Ninth Circuit appears to have imposed a more demanding standard in connection with the interpretation of this safe harbor. The court held that the defendant domain registrant was not entitled to the safe harbor defense because it was unlikely that the registrant legitimately believed that his use of the

domain name at issue was "wholly lawful." 586 F3d at 1203. The defendant had been adjudicated a cybersquatter in other judicial proceedings, and the court found that a reasonable person who had previously been declared a cybersquatter in a judicial proceeding should have known his actions might be unlawful. 586 F3d at 1203.

© The Regents of the University of California

§3.24 b. ACPA Remedies

The remedies under the ACPA are much more extensive than those available under the UDRP. The mark owner has a choice between monetary damages or an injunction. See 15 USC §§1125(d)(1)(A), (C). If monetary damages are elected, the court may grant not less than $1000 and not more than $100,000 per domain name infringement. 15 USC §1117. The only type of remedy in an in rem action is the cancellation of the infringing domain name or transfer of the registration to the mark holder. See 15 USC §1125(d)(2)(D).

© The Regents of the University of California

§3.25 4. Whether to Proceed Under UDRP or ACPA?

A claim should be brought under the UDRP if the claimant would like to resolve the dispute quickly and at low cost (as noted in §3.16, the cost of a UDRP arbitration proceeding is approximately $1500 to $3000). A claim should not be pursued under the UDRP, however, if the claimant is seeking a monetary award or an injunction, because those remedies are not available under the UDRP. As discussed in §3.16, the UDRP only authorizes the arbitration panel to cancel, transfer, or make changes to the infringing domain name.

Because an action under the ACPA must be brought in federal court, it can be fairly expensive and lengthy because of discovery and other federal civil procedures. One advantage of a court proceeding under the ACPA, however, is that the statutory scheme is more developed than the UDRP and the UDRP Rules. Although a proceeding under the UDRP and ACPA may be instituted simultaneously for the same claim, UDRP Rules ¶18 states that the arbitration panel has full discretion to suspend or terminate, or to continue to hear, an administrative proceeding if it is also being heard by a court.

A UDRP proceeding is an administrative remedy exclusive of proceedings under the ACPA. *Barcelona.com v Excelentisimo Ayuntamiento de Barcelona* (4th Cir 2003) 330 F3d 617, 625. The *Barcelona* court noted that while a UDRP panel decision may be the reason for bringing suit in federal court, the UDRP decision is "not given any deference under the ACPA… because a UDRP decision is susceptible of being grounded in principles foreign or hostile to American law." 330 F3d at 626.

© The Regents of the University of California

II. TRADEMARKS, SERVICE MARKS, AND TRADE NAMES

§3.26 A. Introduction

Trademark law can be very important for companies doing business on the Internet. An online business may have many different trademark rights, such as rights in its domain name, graphics, animations, and other visual elements of its website.

Trademarks are subject to both federal and state law. The applicable federal law is the Trademark Act of 1946 (also known as the Lanham Act), 15 USC §§1051-1141n; the federal agency responsible for administering the Lanham Act is the United States Patent and Trademark Office (USPTO). Sections 3.27-3.70 discuss the protections available under federal law for trademarks, service marks, and trade names used on the Internet, federal registration procedures, transferring trademarks, and trademark infringement issues. A trademark need not be registered in order to be valid, but registration brings certain procedural and other advantages that may be substantial and significantly enhances the owner's ability to protect its mark. See §3.30.

If a trademark will be used in only one state, the trademark may be registered at the state level only as an alternative to federal filing. The purpose of state-level registration is to prevent anyone else in the state from using the same mark.

PRACTICE TIP: State-only registration may be adequate for local "bricks and mortar" enterprises or nonprofit agencies that do not do business in interstate commerce, but in most cases would not be appropriate for an Internet-based business.

California law governing trademarks and service marks is in Bus & P C §§14200-14272. The Secretary of State's office maintains registration records and updates of trademarks and service marks registered in California. See §3.31.

The word "mark," as used in the following sections, refers generally to trademarks, service marks, collective marks, certification marks, distinctive trade dress, trade names, and other indicia of the source or ownership of a commercial product or service. For additional discussion of trademarks, see California Business Litigation, chap 6 (Cal CEB 2002). See generally McCarthy, McCarthy on Trademarks and Unfair Competition (4th ed 1996).

© The Regents of the University of California

§3.27 B. Definitions of Trademarks, Service Marks, Collective Marks, Certification Marks, Trade Dress, and Trade Names

Under 15 USC §1127, a trademark is defined as:

> any word, name, symbol, or device, or any combination thereof—(1) used by a person, or (2) which a person has a bona fide intention to use in commerce and applies to register… to identify and distinguish his or her goods, including a unique product, from those manufactured or sold by others and to indicate the source of the goods, even if that source is unknown.

If used to identify and distinguish a service, a mark is referred to as a service mark. Trademarks and service marks are generally treated alike under the Lanham Act. See 15 USC §1053; *Lahoti v VeriCheck, Inc*. (9th Cir 2009) 586 F3d 1190, 1194.

A service is (1) a real activity, (2) performed for the benefit of someone other than the applicant, and (3) different from anything necessarily done in connection with the sale of the applicant's goods or the performance of another service. United States Patent and Trademark Office, Trademark Manual of Examining Procedure (4th ed, Apr. 2005) §1301.01(a) (TMEP), available at http://tess2.uspto.gov/tmdb/tmep. An activity must be identified in connection with use of a service mark that is materially different from what a provider of that particular product or service normally furnishes its customers. *In re Landmark Communications, Inc.* (TTAB 1979) 204 USPQ 692, 695. For example, if an Internet business sells goods online, promotion of those goods would generally not be considered a "service" for trademark law purposes. See *Ex parte Wembley, Inc.* (Comm'r Pats 1956) 111 USPQ 386. In *Wembley,* a manufacturer conducted a national advertising program for its own goods and attempted to obtain trademark protection for the advertising program by categorizing the activity as a "service" to its wholesalers and distributors. The advertising was held not to be a "service" because national product advertising was found to be a normal activity for manufacturers of nationally distributed products. For a service to be registrable as a service mark, the activity must go beyond what is normally expected of a manufacturer in the relevant industry. In *In re U.S. Tobacco Co.* (TTAB 1986) 1 USPQ2d 1502, a tobacco company promoted its goods by sponsoring an automobile race. This activity was held to be an entertainment service under the trademark law because it was outside the scope of what was normally expected of a manufacturer of tobacco products.

A collective mark is a trademark or a service mark used by members of a cooperative, an association, or other collective group or organization, and includes marks indicating membership in a union, association, or organization. 15 USC §1127. A certification mark is any word, name, symbol, or device, or any combination of the foregoing, which is used by a person other than its owner to certify things such region, origin, quality, work and mode of manufacture. 15 USC §1127.

The term trade dress "refers generally to the total image, design, and appearance of a product and may include features such as size, shape, color, color combinations, texture and graphics." *Clicks Billiards, Inc. v Sixshooters, Inc*. (9th Cir 2001) 251 F3d 1252, 1257. For further discussion of trade dress, see §§3.77-3.87.

A trade name or commercial name is defined in 15 USC §1127 as "any name used by a person to identify his or her business or vocation." Trade names are not registrable under federal law unless also used as trademarks, service marks, collective marks, or certification marks. Trade names are protectible, however, under common law principles. See *Academy of Motion Picture Arts & Sciences v Benson* (1940) 15 C2d 685, 104 P2d 650. In California, trade names are generally protected by filing fictitious business name statements in the counties in which the trade name user does business. See Bus & P C §§14411-14418, 17900-17930. See also §3.47.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.28 C. Characterization of Marks

§3.28 C. Characterization of Marks

Under trademark law, marks are characterized as either:

- Coined;
- Arbitrary or fanciful;
- Suggestive;
- Descriptive; or
- Generic.

Two Pesos, Inc. v Taco Cabana, Inc. (1992) 505 US 763, 768, 120 L Ed 2d 615, 112 S Ct 2753. See also *DeGidio v West Group Corp*. (6th Cir 2004) 355 F3d 506, cert denied (2004) 542 US 904. A coined mark is one that is entirely invented and has no inherent relationship to the underlying goods and services (*e.g.,* "KAZAA," for a peer-to-peer file-sharing service). An arbitrary or fanciful mark is a mark that does not describe the product or service, and thus has no logical connection with the product or service. For example, the mark RED RUGS is not arbitrary if it is used as a mark for a manufacturer who sells red rugs, but is arbitrary if it is used in connection with a furniture line. Other examples of arbitrary marks are APPLE and GATEWAY as used in connection with computer products. A suggestive mark is a mark that does relate to the good or service because it characterizes the good or service in some way, but does not clearly convey the nature of the underlying good or service. For example, RED SEA as a mark for hardwood floors may suggest that the color of the hardwood is red, but the floors are not a body of water, thus rendering the mark nothing more than suggestive. See *In re Shutts* (TTAB 1983) 217 USPQ 363 (mark "SNO-RAKE" held to be suggestive and not merely descriptive when used in connection with snow removal tool).

A descriptive mark is one that actually describes a quality, ingredient, or feature of the good or service, or conveys information relating to a quality, ingredient, or feature of the good or service. An example is "Bed and Breakfast Registry," which was found to be a descriptive name for a company engaged in the business of lodging reservations services. See *In re Bed & Breakfast Registry* (Fed Cir 1986) 791 F2d 157. See also *DeGidio v West Group Corp*. (6th Cir 2004) 355 F3d 506, cert denied (2004) 542 US 904 ("LawOffices" as used by plaintiff in domain name held to be descriptive).

The principal criteria for distinguishing a suggestive mark from a descriptive mark is "the imaginativeness involved in the suggestion, that is, how immediate and direct is the thought process from the mark to the particular product." *Lahoti v VeriCheck, Inc*. (9th Cir 2009) 586 F3d 1190, 1198 (citations omitted). A mark is considered suggestive if imagination (or a mental leap) is required to reach a conclusion regarding the nature of the referenced product. In contrast, a mark is descriptive if it "define[s] a particular characteristic of the product in a way that does not require any exercise of the imagination." 586 F3d at 1198 (citations omitted). Lastly, a generic mark uses a common word to describe a product or service, and is usually a noun. For example, RED RUGS would be considered a generic mark if the underlying products were red rugs. The Trademark Trial and Appeal Board in *In re Web Communications* (TTAB 1998) 49 USPQ2d 1478 held that the mark "WEB COMMUNICATIONS" was not registrable because it was a generic term for consulting services to businesses seeking to establish sites on a global computer network. In *America Online, Inc. v AT&T Corp.* (4th Cir 2001) 243 F3d 812, cert dismissed (2001) 534 US 946, the Fourth Circuit affirmed that, as used by AOL, the phrase "You have mail" was a generic term and not a registrable trademark, because it was a common phrase used by the general public and that AOL's usage was within its ordinary meaning, and not distinctive.

The Lanham Act (15 USC §1052(e)(1)) explains that a mark that "merely describes" goods and services associated with a mark is not registrable on the principal register until it acquires secondary meaning. 15 USC §1052(f). The principal register is the primary official list of registered trademarks maintained by the United States Patent and Trademark Office, and, to be registrable on the principal register, a mark must be distinctive. *Kellogg Co. v National Biscuit Co.* (1938) 305 US 111, 118, 83 L Ed 73, 59 S Ct 109; *In re Boston Beer Co. LP* (Fed Cir 1999) 198 F3d 1370. The court in *Boston Beer* upheld the rejection of the mark "Best Beer in America" from the principal register on grounds that it was a mere "laudatory statement" that lacked distinctiveness.

Marks can be categorized from being very distinctive to generic. Coined marks, arbitrary or fanciful marks, and suggestive marks are all inherently distinctive, and thus registrable on the principal register without the need to prove secondary meaning. Descriptive marks must acquire distinctiveness to be eligible for registration on the principal register. Marks that are not sufficiently distinctive to be placed on the principal register may be placed on the supplemental register, unless the marks are unregistrable, as provided in 15 USC §1091(a). For discussion of the advantages of the principal register over the supplemental register, see §3.34.

© The Regents of the University of California

§3.29 D. Priority and Limitations to Priority

In the United States, trademark rights are based on priority of use. See *Sengoku Works Ltd. v RMC Int'l, Ltd.* (9th Cir1996) 96 F3d 1217, 1219, cert denied (1997) 521 US 1103:

> It is axiomatic in trademark law that the standard test of ownership is priority of use. To acquire ownership of a trademark it is not enough to have invented the mark first or even to have registered it first; the party claiming ownership must have been the first to actually use the mark in the sale of goods or services.

The first party to use a mark is the "senior" user and has the right to enjoin "junior" users from using confusingly similar marks in the same industry or market. See *New W. Corp. v NYM Co.* (9th Cir 1979) 595 F2d 1194, 1200. The Lanham Act, however, permits the simultaneous usage of the same or similar marks by two different persons, even if one has priority over the other, if such usage is not likely to confuse consumers. See 15 USC §1052(d). For this reason, rights to a mark may be limited with respect to the types of goods and services sold and the geographic regions where the goods or services are sold.

Acquiring priority to a mark used on the Internet may present a problem for owners of descriptive marks. A descriptive mark is not registrable with the USPTO until it acquires a secondary meaning that makes it distinctive. See 15 USC §1052(f). Traditionally, marks do not acquire a secondary meaning unless they are continuously used in commerce for a long period of time in a substantially exclusive manner, and courts use time as the crucial factor in determining whether the mark has acquired a secondary meaning. See, *e.g., Levi Strauss & Co. v Blue Bell, Inc.* (9th Cir 1980) 632 F2d 817. See also *DeGidio v West Group Corp*. (6th Cir 2004) 355 F3d 506, cert denied (2004) 159 L Ed 2d 268 ("LawOffices" as used by plaintiff in domain name held to be descriptive but not to have acquired a secondary meaning). Examples of descriptive marks that have acquired a secondary meaning include "Raisin Bran" cereal, "Honey Wheat" bread, and the "Yellow Pages." Due to the pace of technological change, marks may gain and lose popularity quickly on the Internet. A mark used on the Internet may not have been used for a sufficient amount of time to acquire distinctiveness. The mark owner can try to establish distinctiveness, however, through a properly conducted consumer perception survey.

© The Regents of the University of California

E. Registration Procedure

§3.30 1. Why Federal Registration?

Trademark rights exist in the absence of federal registration under federal law, state law, or common law. Federal registration, however, typically provides greater substantive and procedural rights than state registration or common law rights based on use alone. The principal benefits of federal registration on the principal register are as follows:

- Registration provides others with constructive notice that the owner of the mark has the right to use the mark on or in connection with the goods or services listed in the registration throughout the entire United States, even if the mark is not being used in a specific geographical area. 15 USC §§1057(c), 1072. Therefore, the registrant can prevent a third party from using the same mark or a confusingly similar mark anywhere in the United States, unless the other mark was used before the date of first use of the registered mark. See §3.29 on priority of use.
- Registration is prima facie evidence that the registered mark is valid; the registrant owns the mark and has the exclusive right to use the mark in commerce subject to any limitations set forth in the certificate. 15 USC §1057(b). See *Lahoti v VeriCheck, Inc*. (9th Cir 2009) 586 F3d 1190, 1199 (fact that mark is registered is strong evidence that mark satisfies statutory requirements for distinctiveness). It is also prima facie evidence that the mark has been used continuously in commerce since the filing date of the application. *Rolley, Inc. v Younghusband* (9th Cir 1953) 204 F2d 209, 211.
- After 5 years of continuous use in commerce, the mark becomes incontestable, and the registration cannot be attacked based on another's prior use or the mark's descriptiveness. 15 USC §1065.
- The registrant of the mark may sue for trademark infringement in federal court. 15 USC §1121(a). (This benefit is also available to registrants under the supplemental register.)
- In a successful trademark infringement action, the registrant may recover attorney fees and has the possibility of recovering treble damages if the infringement is found to be willful. 15 USC §1117.
- The registrant may file its U.S. trademark registration with the U.S. Customs Service to prevent importation of infringing foreign goods. 15 USC §1124.
- The registrant may use the ® symbol in connection with the mark, which may deter potential infringers. 15 USC §1111. (This benefit is also available to registrants under the supplemental register.)
- Registration puts third parties on notice of the registrant's claim of rights in the mark and may deter others from using it in connection with similar goods and services. Deterrence occurs in two ways. First, the U.S. Patent and Trademark Office will generally refuse to register any confusingly similar mark. Second, the mark should appear on the results of trademark searches conducted by businesses that contemplate adopting a mark that is similar. Because most businesses would prefer to use a mark that is not encumbered by the prior rights of a third party, the search results may deter them from using the mark. (This benefit is also available to registrants under the supplemental register.)
- A trademark registration will permit the registrant to take advantage of certain procedural benefits related to cybersquatting and domain name disputes. (This benefit is also available to registrants under the supplemental register.)

© The Regents of the University of California

§3.31 2. Common Law and State Trademark Rights

Common law affords some protection for unregistered trademarks, but trademark rights at common law are not as extensive as the rights granted under federal law for federally registered marks. See §3.30. Like federal trademark rights, common law rights are limited to the scope of the trademark owner's use. At common law, a party who uses a mark without knowledge of the activities of a prior user still has the right to use the mark in a geographical area remote from the areas in which the senior user is operating or to which the senior user is foreseeably likely to expand its operations. For further discussion of common-law trademark rights, see *Hanover Star Milling Co. v Metcalf* (1916) 240 US 403, 60 L Ed 713, 36 S Ct 357; *Rickard v Auto Publisher, Inc.* (11th Cir 1984) 735 F2d 450; and *Southland Corp. v Schubert* (CD Cal 1968) 297 F Supp 477.

California's trademark statutes are at Bus & P C §§14200-14272. In 2007, California adopted the Model State Trademark Act to replace its prior trademark law. Major changes include, *e.g.,* reduction of the term of a California registered trademark from 10 years to 5 years, renewable term for successive 5-year periods (Bus & P C §14217(a)-(b)); expansion of information required with an application for registration of a mark (Bus & P C §14207); and expansion of the grounds for cancellation of a registration (Bus & P C §14230).

The Secretary of State's office maintains records of registrations and updates of trademarks and service marks registered in California. Because registration under state law only grants benefits within the state of California (Bus & P C §§14202(h), 14215(b)), state-level registration is typically sought only if the registrant's use is limited to the state. For trademark registration procedures in California, see http://www.ss.ca.gov/business/ts. Because of the reach of business operations on the Internet, state-only trademark registration is normally insufficient for online businesses. However, state registration combined with federal registration is good insurance that the trademark will be disclosed in any trademark search.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.32 3. Unregistrable Trademarks

§3.32 3. Unregistrable Trademarks

Title 15 USC §1052 identifies the types of marks that cannot be registered on the principal register. See also TMEP §§1203-1207. Under 15 USC §1052(a)-(e), an unregistrable mark is a mark that:

- "Consists of or comprises immoral, deceptive, or scandalous matter; or matter which may disparage or falsely suggest a connection with persons, living or dead, institutions, beliefs, or national symbols, or bring them into contempt, or disrepute; or a geographical indication which, when used on or in connection with wines or spirits, identifies a place other than the origin of the goods and is first used on or in connection with wines or spirits by the applicant on or after" a specified date;
- "Consists of or comprises the flag or coat of arms or other insignia of the United States, or of any State or municipality, or of any foreign nation, or any simulation thereof";
- "Consists of or comprises a name, portrait, or signature identifying a particular living individual except by his written consent, or the name, signature, or portrait of a deceased President of the United States during the life of his widow, if any, except by the written consent of the widow";
- "Consists of or comprises a mark which so resembles a mark registered in the Patent and Trademark Office, or a mark or trade name previously used in the United States by another and not abandoned, as to be likely, when used on or in connection with the goods of the applicant, to cause confusion, or to cause mistake, or to deceive"; or
- Is not registrable unless a secondary meaning is attained, including those that are merely descriptive or deceptively misdescriptive, or primarily geographically descriptive, or merely a surname, and those that comprise any matter that, as a whole, is functional.

Use and misuse of geographic marks is a frequent issue in trademark practice. The Federal Circuit has adopted a three-part test for use in determining whether a trademark is "primarily geographically deceptively misdescriptive" under 15 USC §1052(e)(3). In *In re California Innovations, Inc.* (Fed Cir 2003) 329 F3d 1334, the court held that the amendments to the Lanham Act resulting from the North American Free Trade Agreement (NAFTA) changed the rules under which the PTO may deny registration to misdescriptive marks.

Before NAFTA, there were three categories of geographical marks:

(1) geographically *deceptive* marks that materially deceive the public (§1052(a)), which are permanently unregistrable;

(2) primarily geographically *descriptive* marks (§1052(e)(2)), which are registrable on the Supplemental Register and, if the applicant proves that the mark has acquired distinctiveness, could also be registered on the Principal Register; and

(3) primarily geographically *deceptively misdescriptive* marks (§1052(e)(3)), which were the focus of the *California Innovations* case.

Citing the NAFTA amendments, the Federal Circuit established a three-part test for whether a mark is geographically deceptively misdescriptive and found that such marks would be unregistrable. First, the primary significance of the mark must be a generally known geographic location. Second, the PTO must determine whether the consuming public is likely to believe the place identified by the mark indicates the origin of the goods bearing the mark, when in fact the goods do not come from that place. Finally, the misrepresentation must be a material factor in the consumer's decision of whether to purchase the product. The Federal Circuit cited *In re Save Venice NY, Inc.* (Fed Cir 2001) 259 F3d 1346, a case involving the mark THE VENICE COLLECTION. The court observed that there was "substantial evidence that Venice, Italy is known for glass, lace, art objects, jewelry, cotton and silk textiles, printing and publishing," that "all of applicant's goods are associated with traditional Venetian products," and that "the public would mistakenly believe that they were purchasing 'traditional Venetian products' because the applicant's products were 'indistinguishable' from the products traditionally originating in Venice." 259 F3d at 1354. Therefore, the court found the mark to be unregistrable.

The *California Innovations* case dealt with marks used in connection with goods. A later Federal Circuit decision, *In*

re Les Halles de Paris (Fed Cir 2003) 334 F3d 1371, set forth the test for rejection of geographic marks used in connection with the provision of services. In *Les Halles,* the Federal Circuit recognized that services are different from goods because consumers will usually receive the services at the location of the business, and therefore would be aware that the services are not coming from the geographic location named in the mark. Accordingly, the Federal Circuit required the PTO to provide additional evidence to satisfy the services-place association and materiality prongs of the *California Innovations* test. In service mark cases, the PTO must now show that (a) consumers "will likely be misled to make some meaningful connection between… the service and the relevant place, and (b) there is a 'heightened association' between the service provided and the relevant geographic location." 334 F3d at 1374.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.33 4. Trademark Searches

§3.33 4. Trademark Searches

Registering a mark and defending an infringement lawsuit can be very expensive. Before registering a mark or using it in commerce, it is important to research whether the mark (a) is already registered, (b) is being used in commerce, or (c) is subject to a filed application showing intent to use the mark. See §3.5 for suggestions on how to conduct a search to determine whether use of a mark may infringe another party's rights in a similar mark.

© The Regents of the University of California

§3.34 5. Principal and Supplemental Registers

The U.S. Patent and Trademark Office provides different application forms for registration on the principal register and the supplemental register. See http://www.uspto.gov/teas/eTEASpageA.htm.

The prerequisites for registration on the principal register include the following:

- The mark must already be used in commerce (15 USC §1051(a)(3)(C));
- The mark must identify and distinguish goods or services (15 USC §1052);
- The registration application must be completed and verified as discussed in §§3.38-3.44;
- Generally, the mark must be affixed to the goods, or if affixing the mark is impractical, on documents associated with the goods. If services rather than goods are involved, the mark must be used or displayed in the sale or advertising of the services (15 USC §1127); and
- The mark must not be a designation that is exempt from registration on the principal register under 15 USC §1052 (see §3.32).

Title 15 USC §§1051, 1052, and 1127 constitute the statutory basis for a refusal by the USPTO to register on the principal register subject matter that, due to its nature or the manner in which it is used, does not function as a mark to identify and distinguish the applicant's goods. If a proposed mark is not inherently distinctive, it may be registered on the principal register only on proof of acquired distinctiveness, or "secondary meaning," *i.e.,* proof that it has become distinctive as applied to the applicant's goods or services in commerce. In *Inwood Labs., Inc. v Ives Labs., Inc.* (1982) 456 US 844, 851 n11, 72 L Ed 2d 606, 713 n11, 102 S Ct 2182, the U.S. Supreme Court held that:

> To establish secondary meaning, a manufacturer must show that, in the minds of the purchasing public, the primary significance of a product feature or term is to identify the source of the product rather than the product itself.

Marks that are not eligible for registration on the principal register may be registrable on the supplemental register if they are "capable of distinguishing the applicant's goods or services." 15 USC §1091. Therefore, if a mark does not meet the standards for distinctiveness or secondary meaning required for registration on the principal register, perhaps because the mark is "generic" (see §3.28), it may be possible to obtain registration on the supplemental register. Although the supplemental register does not provide all of the protections and benefits of registration on the principal register, registrants may avail themselves of federal jurisdiction (15 USC §1121(a)) and use the ® symbol in connection with the mark (15 USC §1111). In addition, registration on the supplemental register gives notice to third parties of the registrant's claim to the mark and also provides certain benefits in domain name disputes.

There are several advantages to registering on the principal register rather than the supplemental register, including the following:

- Registration on the principal register constitutes prima facie evidence of the validity of the registered mark and the ownership of the mark (15 USC §1115(a));
- It deters the importation of infringing products or services (15 USC §1124));
- The owner of the mark has the exclusive right to use the mark (15 USC §1115(a)); and
- It provides constructive notice of a claim of ownership (15 USC §1072).

© The Regents of the University of California

§3.35 6. Intent-to-Use Applications

The principal and supplemental registers are only available for marks that are in use. A third category of application, an "intent-to-use application," is available for a business that plans to use a mark but has not yet commenced using the mark in commerce. The Lanham Act provides that an applicant may file an application based on the bona fide intention to use a mark in commerce "under circumstances showing the good faith of such person." 15 USC §1051(b). An intent-to-use application is made on the same form as an application for registration on the principal register.

An intent-to-use application is processed by the USPTO in the same manner as a normal application. It is fully examined, and, when the examining attorney is satisfied that the mark is entitled to registration, it is published for opposition but not registered. See TMEP §1102. Registration of the mark will not occur until a declaration stating that the mark is in use, along with evidence of use, is filed and accepted. 15 USC §1051(c)-(d).

The period of time allowed for filing a declaration of use in an allowed intent-to-use application is initially six months, subject to extension if an effort is being made to put the mark into use in interstate commerce and fees are paid. 15 USC §1051(d); 37 CFR §2.89(e)(1).

There are certain advantages to filing an application on an intent-to-use basis. Subject to the issuance of a registration, an intent-to-use application constitutes constructive use of the mark, effective as of the filing date. Title 15 USC §1057(c) provides that an application to register a trademark confers a nationwide right of priority against any other person except for a person who, prior to such filing, has used the mark. This provision applies to intent-to-use applications because an intent-to-use application is considered an application to register a mark under 15 USC §1051(b). See *Zirco Corp. v American Tel. & Tel.* (TTAB 1991) 21 USPQ2d 1542, 1543. This gives the registrant a nationwide right of priority in the mark for the specified goods or services over all subsequently filed applications and subsequent users of the mark on similar goods or services. *WarnerVision Entertainment v Empire of Carolina, Inc.* (2d Cir 1996) 101 F3d 259.

Unlike a use-based application, an intent-to-use application claiming more than one class of goods or services may be divided so that the registrant need not wait for the mark to be used in connection with all intended classes of goods and services before obtaining registration. The rights can be "taken down" as the use of the mark rolls out over time. The application for registration in connection with the other goods and services would still remain pending. 37 CFR §2.87. See also TMEP §1110.

Because the most common form of trademark registration application is an application for registration on the principal register, §§3.36-3.44 focus on the procedures and requirements for use-based applications for registration of marks intended for the principal register.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.36 7. Form of Application

§3.36 7. Form of Application

Applications for registration can be filed electronically on the USPTO's Trademark Electronic Application System, using the function called "e-TEAS," or by downloading and printing the application form off of the USPTO website (using the function called "PrinTEAS") and mailing it to the USPTO. Both e-TEAS and PrinTEAS are relatively easy to use, by following the online instructions for each function posted at the USPTO website. See http://www.uspto.gov/teas.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.37 8. Application Procedure

§3.37 8. Application Procedure

When the USPTO receives an application, an examining officer reviews it and initially determines if the application contains all the necessary components. Many applications are rejected at this stage of the process because they are incomplete. If the application is accepted, the USPTO assigns the application a serial number to identify the mark. TMEP §401.01.

© The Regents of the University of California

§3.38 9. Contents of Application

An applicant for registration must submit an application, a verified statement, the prescribed filing fee, and specimens of the mark as used in commerce. 15 USC §1051(a)(1). See §§3.39-3.44. The specimen must demonstrate a direct link between the mark and the services for which the proposed mark will be used. See *In re DSM Pharms., Inc.* (TTAB 2008) 87 USPQ2d 1623. The application must include the applicant's domicile and citizenship, the date of the applicant's first use of the mark, the date of the applicant's first use of the mark in commerce, a description of the goods in connection with which the mark is used, and a drawing of the mark. 15 USC §1051(a)(2). If the applicant is aware of a concurrent use of the mark by another, the applicant must specify, to the extent of his or her knowledge, each such concurrent use, the goods on or in connection with which and the geographical areas in which each such concurrent use exists, the periods of each use, and the goods and area for which the applicant desires registration. 15 USC §1051(a)(3)(D). See §3.40.

For further information regarding the contents of registration application, see §§3.39-3.44. See also the checklist provided in TMEP §818.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.39 a. Applicant Information

§3.39 a. Applicant Information

The application must be filed by the owner of the mark. 15 USC §1051(a)(1). The applicant must be a natural person or a corporation, partnership, joint venture, union, association, or any other type of entity that can sue and be sued. In addition, the application must state the citizenship of the applicant or the state or nation under whose laws the applicant is organized, and the applicant's address. 15 USC §1051(a)(2), (b)(2).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.40 b. Verification

§3.40 b. Verification

Each application must include a verified statement specifying that (15 USC §1051(a)(3)):

- The verifier believes that he or she, or the entity on whose behalf the verification is made, is the owner of the mark for which registration is sought;
- To the best of the verifier's knowledge and belief, the facts recited in the application are accurate;
- The mark sought to be registered is in use in commerce; and
- To the best of the verifier's knowledge and belief, no one else has the right to use the mark in commerce in an identical form or in a form that is likely to cause confusion or mistake or to deceive.

If the mark is being used by another person or entity, an applicant may request issuance of a registration despite the pre-existing rights of a third party in a conflicting mark under 15 USC §1052(d). This is called a "concurrent use" application. In a concurrent use application, the applicant typically seeks registration for a specified limited geographical area and lists one or more parties who have rights in the mark in other geographical areas of the United States. See *Holiday Inn v Holiday Inns, Inc.* (CCPA 1976) 534 F2d 312; *Thriftimart, Inc. v Scot Lad Foods, Inc.* (TTAB 1980) 207 USPQ 330. In the case of a concurrent use application, additional verifications are required. See 15 USC §1051(a)(3)(D).

© The Regents of the University of California

§3.41 c. Identification and Classification of Goods and Services; Filing Fees

An application must contain a concise statement of the particular goods or services that are used in connection with the mark, and the classification number applicable to those goods or services under the International Schedule of Classes of Goods and Services. 37 CFR §2.32(a)(6). The International Schedule of Classes of Goods and Services can be found at http://www.uspto.gov/web/offices/tac/doc/basic/international.htm. As an aid to interpreting the Schedule, the USPTO has published the Trademark Acceptable Identification of Goods and Services Manual, available at http://tess2.uspto.gov/netahtml/tidm.html, which is an official list of goods and services to be used in identifying the service or product stated on the application, and of the classifications of such services or products.

Identifying the goods or services correctly becomes very important in a dispute with a competing mark owner. If a competing mark owner asserts that the proposed mark is confusingly similar to the competitor's mark in connection with the goods or services being provided, an accurate and concise description of the goods or services may allow the proposed mark owner to differentiate its mark from the other mark based on the fact that different goods or services are registered under its mark. Importantly, once a description of the goods or services is filed with the application, it may be amended only to clarify or narrow the description of the goods or services. Title 37 CFR §2.71(a) precludes additions to the identification of goods or services by amendment to an application for registration. A separate new application must be filed for additional classes.

PRACTICE TIP: When registering a mark to be used on the Internet, consider all of the applicable goods and services connected with the mark. A mark is typically protected to the extent that the certificate of registration for a concurrent or similar mark does not list the same goods or services as the other mark. Accordingly, to obtain the broadest trademark rights, the application for registration should list all possible goods and services in connection with which the mark is used. For example, the owner or operator of an online celebrity fan club can potentially register several different classes of services in connection with the mark used by the fan club. If the fan club sells merchandise and provides online chat rooms and similar services, then the application for registration should list separate classifications for selling merchandise and for providing online chat-room services.

Trademark filing fees are paid based on the number of classes claimed in the application. 15 USC §1112. Current fees are set forth in 37 CFR §2.6; the fee for filing an application with the USPTO is presently $375 per class for paper filings and $325 per class if using the USPTO's online filing system, Trademark Electronic Application System (TEAS).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.42 d. Bases for Filing

§3.42 d. Bases for Filing

For a mark to be approved for publication and registration, the application for registration must specify one of the following four bases for filing:

- Use of the mark in commerce, under 15 USC §1051(a);
- Intent to use the mark in commerce, under 15 USC §1051(b);
- Registration of a mark in a foreign applicant's country of origin, under 15 USC §1126(e); or
- A claim of priority, based on an earlier-filed foreign application, under 15 USC §1126(d).

More than one basis can be asserted for each good or service involved. After filing an application, one may change the filing basis unless the mark has been published. The following is a summary of the requirements of the first two, and most common, bases for filing:

- *Use in commerce*. Use-in-commerce applications must include the following: (1) a verification by the mark owner that the mark is used in commerce on or in connection with the goods or services listed on the application (if a verification statement is not sent with the application, the statement must assert that the mark was used in commerce on or in connection with the goods or services listed in the application as of the application filing date); (2) the date that the applicant first used the mark; (3) the date that the designation was first used in commerce as a trademark or service mark (if the designation has been used in connection with more than one good or service, only one date should be listed); and (4) a specimen showing how the applicant actually uses the mark in commerce. See also 15 USC §1051(a).
- *Intent to use*. In an intent-to-use application, the mark owner must verify that he or she has a bona fide intent to use the mark in commerce on or in connection with the goods or services listed in the application. If the verification is not filed with the initial application, the applicant must state that the applicant had a bona fide intent to use the mark in commerce as of the filing date of the application. The application may list more than one good or service as long as the applicant has a bona fide intent to use the mark in commerce on or in connection with each good or service listed. See also 15 USC §1015(b).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.43 e. Drawing Requirement

§3.43 e. Drawing Requirement

The applicant must submit a drawing of the mark with the original application to receive a filing date, unless the application is for the registration of sound, scent, and other nonvisual marks. See 15 USC §1051(a)(2), (b)(2); TMEP §807. For registrations of sound, scent, and other nonvisual marks, the applicant must submit a written description of the mark explaining the sound, smell, or nonvisual nature of the mark. A drawing provides notice of the mark being registered, and is available to the public through the Trademark Electronic Search System (known as "TESS") on the USPTO website at http://www.uspto.gov/main/trademarks.htm. The drawing must comply with specified requirements concerning the type of paper, heading, and size of the drawing. See TMEP §807.01.

If the mark contains colors, the applicant may show the drawing either in black and white or in colors in the drawing specimen. The USPTO does not publish marks in color, however, so a black and white drawing must be submitted before the mark is approved for publication or for registration.

Some marks may also include motion, in which case the applicant may submit a drawing that contains up to five freeze frames showing various points in the movements, and a detailed written description of the mark must also be submitted. 37 CFR §2.52(b)(3).

NOTE: Amendments of a drawing are not allowed if the amendment materially alters the mark. 37 CFR §2.72.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.44 f. Description of Mark

§3.44 f. Description of Mark

An examining attorney may require that the applicant provide additional written descriptions of a graphic mark. Any application not presented in standard characters must include a description of the mark. 37 CFR §2.37. A description is also usually required when:

- A significant element of a mark is unclear or ambiguous;
- The mark is three-dimensional, or consists of a configuration of the goods or packaging;
- The drawing includes broken lines to show placement or to indicate that a portion of the product or packaging is not part of the mark;
- The mark includes color;
- The mark includes motion; or
- The mark is a sound, scent, or nonvisual mark.

TMEP §808.01. Marks that include non-English words must include a translation of the words. TMEP §809. Marks will be evaluated based on their English language equivalents. Therefore, a mark in a foreign language that has the same meaning as a pre-existing English-language mark may be subject to rejection due to likelihood of confusion. See *Ex parte Odol-Werke Wien Gesellschaft M.B.H*. (Comm'r Pats 1956) 111 USPQ 286 (registration of mark, "Chat Noir," was refused because English language equivalent, "Black Cat," was already registered as trademark for related goods).

© The Regents of the University of California

10. Registration of Domain Names as Trademarks

§3.45 a. Requirements

A domain name is registrable as a trademark or service mark if it is used as a trademark or service mark. If the domain name is a company's trade name, and it also is used as a trademark, then the trade name also is registrable as a trademark. To serve as a trademark, the domain name must do more than simply provide an "address" for an Internet site. It must also indicate the source of a product or service. *In re Eilberg* (TTAB 1998) 49 USPQ2d 1955. In the *Eilberg* case, the Trademark Trial and Appeal Board (TTAB) held that a designation that serves only to identify the applicant's domain name or its location on the Internet, and does not identify the applicant's services, does not in and of itself function as a service mark. The applicant's proposed mark, http://www.eilberg.com, was used in connection with providing legal services. The designation was used on the applicant's letterhead and business cards. The TTAB explained that it would have decided differently if the name of the law firm was in fact "eilberg.com".

It is not clear whether the suffix of a domain name, also called the top level domain name (TLD), is registrable. In 1999, the USPTO released Examination Guide No. 2-99, *Marks Composed, in Whole or in Part, of Domain Names* (USPTO, Sept. 29, 1999), referred to in this chapter as "Guide No. 2-99" and available at http://www.uspto.gov/web/offices/tac/notices/guide299.htm. Guide No. 2-99 explained that the TLD ".com" adds nothing to the distinctiveness of the designation as a trademark or service mark and thus need not be included when registering the domain name as a mark. The USPTO analogized the TLD to a nondistinctive part of a telephone number such as "800." There is no absolute prohibition against including a TLD, because it may become an important part of a mark. In most cases, however, the USPTO is likely to require the trademark registration owner to disclaim exclusive rights to the TLD portion of the mark.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.46 b. Reasons for Refusal of Registration of Domain Names

§3.46 b. Reasons for Refusal of Registration of Domain Names

As indicated in §3.45, the USPTO will reject an application to register a domain name as a mark if the domain name is not in fact used as a mark. When choosing a domain name, it should be noted that the following types of domain names are likely to be refused registration as a trademark by the USPTO (see Examination Guide No. 2-99):

- A domain name that is created only to advertise products;
- A domain name to be used only as an Internet address;
- A proposed mark containing a surname and a top-level domain name (TLD) such as ".com";
- A proposed mark composed only of descriptive terms and a TLD, such as "nationalclothingoutlet.com" for clothing store services;
- A proposed mark that is composed of a generic term for an applicant's goods and services and a TLD, such as "eyeglasses.com" for a website that sells eyeglasses;
- A proposed mark containing a geographic description such as LosAngeles.com; and
- A proposed mark that includes the phonetic equivalent of a TLD (*e.g.,* abrahamsmortgagedotcom.com or jacquelinejeweldotcom.com). Such marks are likely to be rejected and are treated the same way as a regular TLD that is included in a proposed mark.

© The Regents of the University of California

§3.47 11. Trade Names

A trade name may not be registrable as a trademark if it functions only to identify the name of a business. 15 USC §§1051-1052, 1127. If the trade name also identifies a product or service, however, then it may be registrable. See *In re Walker Process Equipment Inc.* (Comm'r Pats 1954) 102 USPQ 443, aff'd (CCPA 1956) 233 F2d 329. For example, if an online business has a domain name that is different from its corporate name, and markets and sells products to the public through its website solely under its domain name, it is likely a court would find the corporate name to be a trade name rather than a trademark because the business is not using its corporate name to identify the source of its goods or services. The domain name—the name under which the company markets its products—is likely to be treated as the company's trademark.

© The Regents of the University of California

§3.48 F. Madrid Protocol

United States trademark owners can use the Protocol Relating to the Madrid Agreement Concerning the International Registration of Marks (June 27, 1989) (see 15 USC §§1141-1141n), referred to as the "Madrid Protocol," to obtain trademark protection in countries that have adopted it by filing only one trademark application with the USPTO. For further information, see http://www.uspto.gov/web/trademarks/madrid/madridindex.htm and the Madrid Protocol Implementation Act, codified at 15 USC §§1141-1141n. A copy of the Madrid Protocol is available at http://www.wipo.int/madrid/en.

There are many benefits to the Madrid Protocol, one of which is that only one application is necessary to obtain trademark protection in multiple countries, which greatly reduces the overall cost of registering marks for worldwide use. Madrid Protocol, art 2. Another benefit is that the Madrid Protocol requires an application for registration to be acted on within 18 months of its submission. Madrid Protocol, art 5. The Madrid Protocol also gives applicants priority as provided for in the Paris Convention, which is generally the date the applicant files for trademark registration under the Madrid Protocol in the applicant's national office. Madrid Protocol, art 4; Paris Convention for the Protection of Industrial Property of March 20, 1883, art 4. The Paris Convention can be found at http://www.uspto.gov/web/offices/pac/mpep/documents/appxp.htm.

Generally, to use the Madrid Protocol, one must already have a trademark application or registration in the applicant's national office. Once the applicant files the necessary documents required by its national office to request protection under the Madrid Protocol indicating for which of the participating jurisdictions trademark registration is sought, the applicant's national office will then submit an application on behalf of the applicant to the World Intellectual Property Organization (WIPO). At that time, WIPO determines whether the filing requirements are met. If the requirements are met, WIPO will register the mark and publish it in the WIPO Gazette of International Marks. Madrid Protocol, art 3.

Before the United States adopted the Madrid Protocol, separate trademark registration applications were needed in each jurisdiction, which usually required the engagement of multiple local counsel. The effect of the Madrid Protocol has been to expedite significantly the procedures for international trademark registration.

© The Regents of the University of California

G. Grant or Denial of Registration

§3.49 1. Opposition, Cancellation, or Registration

Under 15 USC §1063, persons who believe that they would be damaged by the registration of a mark on the principal register may file an opposition to a trademark application with the USPTO. The complainant must assert that (1) the complainant's mark is likely to be damaged by a registration of the applicant's mark, and therefore the complainant has standing to oppose registration of the contested mark, and (2) there is a valid basis for barring the applicant from registering the mark (such as the likelihood of confusion between conflicting marks or an underlying defect in the mark itself such as descriptiveness). A notice of opposition must be filed along with a fee within 30 days from the date that the application is published in the USPTO's Official Gazette, but extensions of time to file the opposition may be obtained. See 15 USC §1063. Because of the relatively short period of time within which trademark applications can be opposed, trademark owners should consider monitoring the Official Gazette on a periodic basis to ensure that timely oppositions can be made as necessary.

Marks on the supplemental register are not published in the Official Gazette and thus cannot be opposed. Instead, those desiring to contest a mark must pursue cancellation proceedings. 15 USC §1064.

If no opposition proceedings have been instituted and the application meets statutory and regulatory requirements, the examining attorney will approve the application, and the mark will be entitled to registration on the principal register. The mark is then registered in the USPTO and a certificate of registration is issued. 37 CFR §2.151. If the applicant applied for registration under an intent-to-use application under 15 USC §1051(b), a notice of allowance is issued and the applicant must submit a statement of use before the registration will be issued. See §3.42.

NOTE: Any person who believes that he or she is or will be damaged in any way, including as a result of dilution, may petition the Trademark Trial and Appeal Board to cancel a registered mark within five years from the date of the registration of the mark on the principal register. 15 USC §1064(1). In addition, an action for cancellation of a mark may be brought at any time if the registered mark (1) becomes the generic name for the goods or services, (2) has been abandoned, (3) was obtained fraudulently, or (4) is being used by, or with the permission of, the registrant to misrepresent the source of the goods or services on or in connection with which the mark is used. 15 USC §1064(3).

© The Regents of the University of California

§3.50 2. Appeals From Denials of Registration

If the examining attorney denies registration, an appeal may be taken to the Trademark Trial and Appeal Board (TTAB). 15 USC §1070. An applicant may appeal to the TTAB within six months after the examiner's final decision by filing a notice of appeal and paying a fee. Within 60 days after initiating an appeal, the applicant must file an appeal brief. The examining attorney will also file an appeal brief to which the applicant may file a reply brief within 20 days. 37 CFR §2.142(b). The appellant may request an oral argument. 37 CFR §2.142(e). See TMEP §1501 for a more complete description of TTAB appeal procedures. An applicant who is dissatisfied with the decision of the TTAB may appeal to the U.S. Court of Appeals for the Federal Circuit. 37 CFR §2.145.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.51 H. Use of Trademark Symbol

§3.51 H. Use of Trademark Symbol

Before issuance of a federal trademark registration, the trademark owner can use the symbol in connection with the mark to put third parties on notice of its assertion of ownership rights. TMEP §906. Once the mark is registered in the USPTO, the mark owner may give notice of its registration by displaying the symbol ® or the phrase "Registered in U.S. Patent and Trademark Office" or "Reg. U.S. Pat. & Tm. Off" with the mark. 15 USC §1111. Under 15 USC §1111, if a mark owner fails to give notice of registration in this manner, the owner cannot recover profits and damages under the Lanham Act for infringement unless the infringer had actual notice of the registration.

PRACTICE TIP: Using either the ® symbol or one of the phrases mentioned above before registration with the USPTO may bring negative consequences in subsequent litigation, such as (1) denial of injunctive and monetary relief (see *Urecal Corp. v Masters* (ND Ill 1976) 413 F Supp 873); (2) exposure to a counterclaim for false advertising under 15 USC §1125(a) (see *Sports Auth., Inc. v Abercrombie & Fitch* (ED Mich 1997) 965 F Supp 925); and (3) a third party challenge to the mark's initial registration (see *Wells Fargo & Co. v Lundeen & Assocs*. (TTAB 1991) 20 USPQ 2d 1156).

© The Regents of the University of California

§3.52 I. Duration and Renewal

Generally, a registered mark is protected under the Lanham Act for a period of 10 years after the date of registration. 15 USC §1058(a). To renew the registration, the owner of the mark must pay a fee and file an affidavit within the one-year period preceding the end of the current registration period. 15 USC §1058(b). The affidavit must set forth, among other things, that the goods or services used in connection with the mark (1) are used in commerce (the USPTO may require specimens or facsimiles proving the current use of the mark) or (2) are not used in commerce but that such nonuse is due to special circumstances that excuse such nonuse of the mark, and is not due to any intent to abandon the mark. 15 USC §1058(b). There is a grace period of 6 months after the expiration of the 10-year period to file an affidavit of renewal. 15 USC §1058(c).

© The Regents of the University of California

§3.53 J. Preservation of Trademark Rights

Businesses should take steps to preserve their trademark rights by protecting the value, significance, and distinctiveness of their marks. They should adopt formal policies prescribing the allowable uses of the mark by employees, licensees (if any), and any other persons or entities who have access to the mark. Model trademark policy guidelines are set forth in §3.55. It is important to preserve a mark's significance so that it will not be considered abandoned. If a mark is abandoned, it enters the public domain where it can be freely used by anyone. *Moore Bus. Forms v Ryu* (5th Cir 1992) 960 F2d 486, 489; *Taco Cabana Int'l, Inc. v Two Pesos, Inc.* (5th Cir 1991) 932 F2d 1113, aff'd (1992) 505 US 763; *Kentucky Fried Chicken Corp. v Diversified Packaging Corp.* (5th Cir 1977) 549 F2d 368. The question of whether abandonment has occurred is normally an issue of fact.

A mark is deemed to be "abandoned" if either of the following occurs (15 USC §1127):

- When its use has been discontinued with intent not to resume such use. Intent not to resume may be inferred from circumstances. Nonuse for three consecutive years is prima facie evidence of abandonment. "Use" of a mark means the bona fide use of such mark made in the ordinary course of trade, and not made merely to reserve a right in a mark.
- When any course of conduct of the owner, including acts of omission as well as commission, causes the mark to become the generic name for the goods or services on or in connection with which it is used or otherwise to lose its significance as a mark. Purchaser motivation is not a test for determining abandonment in this context.

There are several ways a mark may be abandoned unintentionally. Abandonment may occur if a licensor does not restrict use of a licensed mark by the licensee. If a licensee uses a mark without restriction (a "naked license"), the mark can lose its significance, and consequently its distinctiveness. *Dawn Donut Co. v Hart's Food Stores, Inc*. (2d Cir 1959) 267 F2d 358, 367. See also *Barcamerica Int'l v Tyfield Importers, Inc.* (9th Cir 2002) 289 F3d 589. A mark may also be considered abandoned if it loses its distinctiveness and becomes a generic term. 15 USC §1127. Lastly, if a mark is changed, or amended in such a way that the public is unable to recognize it, it may be considered abandoned. *Moore Bus. Forms v Ryu* (5th Cir 1992) 960 F2d 486.

© The Regents of the University of California

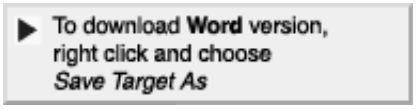
§3.54 K. Trademark Licensing

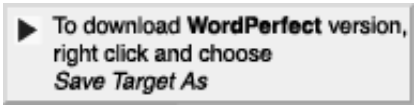
Because a mark is considered intangible personal property, it may be assigned, sold, and licensed. As noted in §3.53, however, when licensing, the mark owner should prevent unrestricted uses of the mark by the licensee so that the mark will not risk being considered abandoned or diluted. Thus, when drafting a licensing agreement, the attorney should be careful to include provisions that restrict usage and require monitoring and periodic reporting on usage of the mark. The trademark guidelines set forth in §3.55 contain sample provisions that restrict uses of a licensed mark, and may be helpful in establishing restrictions for employees and other persons. The guidelines are designed to be used in conjunction with a trademark license agreement, a form of which is provided in §3.56, and certain defined terms in the guidelines, such as "Licensed Marks" and "Licensee," are defined in the license agreement. Assignments of trademarks are addressed in §§3.57-3.59.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.55 1. Form: Trademark Guidelines

§3.55 1. Form: Trademark Guidelines





TRADEMARK GUIDELINES OF _ _[*NAME OF COMPANY*]_ _

NO ALTERATIONS. Licensee shall not change or modify the Licensed Marks, or create any design variation of the Licensed Marks, in any advertising, marketing, distribution, or sales materials, or any other materials, without obtaining the prior written consent of _ _[*name of company*]_ _ (the "Company").

NO COMBINATIONS. Licensee shall not, without the prior written consent of the Company, join any name, domain name, mark, or logo with the Licensed Marks so as to form a composite trade name, mark, or domain name.

IMPROPER APPEARANCES. Licensee shall not knowingly use any of the Licensed Marks in any manner that might reasonably be expected to tarnish, disparage, or reflect adversely on any of the Licensed Marks or the goodwill associated with the Licensed Marks or the Company.

SIMILAR MARKS. Licensee shall not seek to adopt as a trademark, service mark, trade name, domain name, or other designation any word, symbol, or other form of identification that is the same as or confusingly similar to any of the Licensed Marks (a "Similar Mark"). In addition to constituting a breach of the License Agreement into which these guidelines are incorporated (the "Agreement"), the use of any such Similar Mark shall be deemed to be for the benefit of Company and all right, title, and interest in and to any Similar Mark, together with all goodwill thereof, shall belong exclusively to Company. If Licensee desires to adopt a Similar Mark, it shall advise Company in writing and Company, in its sole discretion, shall decide if it desires to adopt such Similar Mark.

COMPLIANCE WITH LAW. Licensee shall use the Licensed Marks only in such manner as shall comply with the provisions of applicable laws and regulations relating to the Licensed Marks.

CONTINUOUS USE. Licensee shall start using the Licensed Marks not later than _ _[*date*]_ _. Thereafter, Licensee shall use all Licensed Marks on a continuous basis. Licensee shall use any new marks of the Company as soon as practical after the date that such new marks are licensed to Licensee. Licensee shall not allow any material discontinuation of use that would result in the abandonment of any of the Licensed Marks during the term of the Agreement without first obtaining Company's written consent to such discontinuation of use.

NOTICES. Licensee shall affix to all materials that bear a Licensed Mark (a) notices in compliance with applicable laws, including without limitation, trademark laws, and (b) such legend as Company may reasonably designate by written notice that is required or otherwise reasonably necessary to allow adequate protection of the Licensed Marks and to enable Company to claim the benefits thereof under applicable laws, including without limitation, trademark laws. All materials shall be deemed to include, but are not limited to, all Web pages located within the Company's Website, stationery, labels, packaging, advertising and promotional materials, manuals, invoices, and all other printed materials.

NO CONTEST. Licensee acknowledges and admits the validity of the Licensed Marks. Licensee covenants that it shall not, directly or indirectly, challenge the validity of the Licensed Marks, or any registrations thereof and/or applications therefor in any jurisdiction, or the right, title, and interest of Company and _ _[*names of affiliated entities*]_ _ therein and thereto, nor shall it claim any interest in the Licensed Marks in any jurisdiction, other than the rights expressly granted hereunder.

QUALITY STANDARDS. The Licensed Marks shall at all times be used and produced, as the case may be, only in accordance with such quality standards and specifications as Company may establish and communicate to Licensee from time to time.

IMPROPER USE. Licensee shall not use the Licensed Marks in any way that could reasonably be expected to adversely affect or otherwise denigrate or disparage the Company's brand, image, or rights to the Licensed Marks, or the goodwill associated therewith.

DESIGN. Company shall have the right to approve or disapprove the design and use of the Licensed Marks or the Company's name on any page on which either appears within the Company Website, including any "look and feel" issues that adversely affect the presentation of the Licensed Marks or of the Company's name. In addition, Company shall have the right to determine whether the Licensee's site conforms or fails to conform as Company may determine necessary in its sole, good faith opinion to maintain the validity and enforceability of the Licensed Marks and to protect the goodwill associated therewith.

APPEARANCE. All use of the Licensed Marks made by Licensee hereunder shall faithfully reproduce the design and appearance of the Licensed Marks as reflected in the documentation provided by Company to Licensee.

PERIODIC INSPECTION AND APPROVAL. Company shall have the right to inspect and approve any and all uses of the Licensed Marks by Licensee, which approval shall not be unreasonably withheld.

COMPANY CHANGES. Licensee shall make such changes to the use of the Licensed Marks as Company may request to maintain the validity and enforceability of the Licensed Marks and to protect the goodwill associated therewith. If Company decides, for reasons relating to trademark or copyright law, that it is commercially necessary to cease use of or modify a Licensed Mark, Company shall so notify Licensee in writing. Licensee shall make best efforts to follow the instructions contained in the notice.

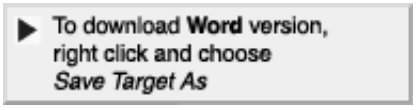
TRADEMARK DISPUTES. In no event shall Licensee enter into any agreement, offer to pay any money to any third party as a settlement, royalty, or license fee, or otherwise resolve a trademark dispute without Company's prior written consent.

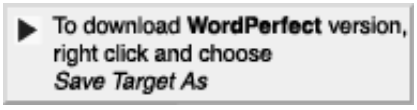
RECORDS. Licensee shall assist Company in protecting the Licensed Marks by keeping records of Licensee's use of the Licensed Marks. Accordingly, during the term of the Agreement and for a period of 2 years after it expires or is terminated, Licensee shall maintain records sufficient to identify all uses of the Licensed Marks by Licensee. These records shall include, but not be limited to, specimen copies of all written materials on which any of the Licensed Marks appear, marked to show the dates and manner of their use and distribution.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.56 2. Form: Trademark License Agreement

§3.56 2. Form: Trademark License Agreement





TRADEMARK LICENSE AGREEMENT

THIS AGREEMENT, effective as of _ _[*date*]_ _, is by and between _ _[*name of company*]_ _, a _ _[*state of incorporation*]_ _ corporation, with an address of _ _[*address of company*]_ _ ("Licensor"), and _ _[*name of licensee*]_ _, a _ _[*state of incorporation*]_ _ corporation, with an address of _ _[*address of licensee*]_ _ ("Licensee").

WHEREAS, Licensor is the owner of the name and mark _ _[*name of trademark*]_ _; and

[*If there is a registration, add before "; and"*]

and is the owner of United States trademark/service mark Registration No. _ _[*registration number*]_ _ of said mark

[*Continue*]

WHEREAS, it is the mutual desire and intention of the parties that Licensee be authorized and permitted by Licensor to use the mark _ _[*name of licensed mark*]_ _ (the "Licensed Mark") in connection with _ _[*describe goods/services*]_ _ (the "Licensed Goods") in the manner and subject to the terms and conditions set forth in this Agreement.

NOW, THEREFORE, in consideration of the premises and the mutual covenants of the parties set forth below and other good and valuable consideration, the sufficiency of which is hereby mutually acknowledged, the parties agree as follows:

1. GRANT OF LICENSE. Licensor grants to Licensee _ _[*a nonexclusive/an exclusive*]_ _ license to use the Licensed Mark in connection with the Licensed Goods in the following geographic areas: _ _[*describe areas*]_ _. The license shall bear royalties. The applicable royalties and payment terms are attached hereto as Exhibit A and incorporated herein by this reference.

2. NO ASSIGNMENT. The license to use the Licensed Mark may not be assigned or otherwise transferred by Licensee without the prior, express, written consent of Licensor.

[*If applicable, add*]

Licensor does not grant, and nothing in this Agreement shall be construed as granting, to Licensee the right to license, sublicense, or authorize others to use the Licensed Mark.

3. USE OF THE LICENSED MARK. Licensee shall use the Licensed Mark solely in connection with the Licensed Goods. Licensee shall always use the Licensed Mark on and in connection with the Licensed Goods in a style or size of print distinguishing it from any accompanying wording or text, at least where the Licensed Mark is most prominently displayed on any printed or other materials used in connection with the advertising and sale of the Licensed Goods.

[*If the mark has a federal registration, add*]

Licensee shall display the federal registration symbol ® to the right of and slightly above the last letter of the Licensed Mark.

[*If the mark does NOT have a federal registration, add instead*]

After grant of a federal registration of the Licensed Mark to Licensor, Licensee shall display the federal

registration symbol ® to the right of and slightly above or below the Licensed Mark where it is most prominently displayed on materials used in the advertising and sale of the Licensed Goods.

[*Continue*]

On termination of this Agreement in any manner provided herein, Licensee shall permanently discontinue all use of the Licensed Mark and refrain from using any other service mark, trademark, trade name, corporate name, or any other designation confusingly similar to the Licensed Mark.

4. QUALITY CONTROL. Licensee's use of the Licensed Mark and the nature and quality of the Licensed Goods sold by Licensee under the Licensed Mark shall at all times comply with Licensor's standards and specifications, which shall be provided by Licensor to Licensee and may be updated by Licensor from time to time on 30 days' written notice to Licensee.

Licensee shall permit duly authorized representatives or agents of Licensor at all reasonable times to inspect materials used by Licensee in the manufacture and sale of the Licensed Goods under the Licensed Mark and all other records relating to the quality of such goods.

Licensee shall provide Licensor with proofs of materials used in the advertising and sale of the Licensed Goods under the Licensed Mark for approval by Licensor before the use thereof, which approval shall not be unreasonably withheld or delayed. Such approval shall be assumed granted if Licensee does not receive written advice to the contrary within 15 days after the date Licensee sends such materials to Licensor.

If the Licensed Goods manufactured and sold under the Licensed Mark and/or any materials used by Licensee in the advertising and sale of the Licensed Goods do not meet Licensor's quality standards as reasonably determined by Licensor, which determination shall be given by Licensor to Licensee in writing, Licensee shall not use the Licensed Mark in any manner on or in connection with the Licensed Goods; provided, however, that if Licensee, within 60 days after receiving that written notification from Licensor, cures or otherwise corrects such failure to meet Licensor's quality standards to Licensor's reasonable satisfaction, Licensee shall be entitled to continue its use of the Licensed Mark in connection with the Licensed Goods.

5. OWNERSHIP. Licensee acknowledges that the Licensed Mark is valid, is the exclusive property of Licensor, and can lawfully be used only with the express license or consent of Licensor. Licensee shall not at any time do, or cause to be done, any act or thing contesting or in any way impairing or intending to impair the validity of the Licensed Mark and/or Licensor's exclusive rights, title, and interest in and to the Licensed Mark.

Licensee shall not register or apply to register the Licensed Mark, either alone or in combination with any other word(s) and/or design(s), in any country, state, or jurisdiction. Licensee shall not in any manner represent that it owns the Licensed Mark, and Licensee hereby acknowledges that its use of the Licensed Mark shall not create any rights, title, or interest in or to said mark in Licensee's favor, but that all use of the Licensed Mark by Licensee shall inure to the benefit of Licensor.

6. TERMINATION. Unless sooner terminated under the provisions of this Paragraph, or by agreement of the parties in writing, this Agreement shall continue in full force and effect for a term of _ _[*number of years*]_ _ years, and may be renewed for such additional terms as Licensor and Licensee may agree on in an instrument in writing duly executed by both parties.

If Licensee materially violates or fails to comply with any of the provisions of this Agreement, Licensor may terminate this Agreement by express written notice to Licensee; provided, however, that if Licensee, within 60 days after Licensor's notice, cures or otherwise corrects such violation or noncompliance to Licensor's reasonable satisfaction, said termination notice shall be of no further force or effect and this Agreement shall be reinstated under all the terms and conditions as existed before the notice of termination.

7. INDEMNITY. Other than the provisions in this Agreement, Licensor assumes no liability to Licensee or to third parties with respect to the Licensed Goods manufactured and sold by Licensee under the Licensed Mark.

Licensee shall indemnify and defend Licensor against any loss or losses incurred through claims, actions, or lawsuits by third parties against Licensor involving or arising from the Licensed Goods manufactured and sold by Licensee under the Licensed Mark, and shall hold Licensor harmless for any damages, attorney fees, or other costs that Licensor may be required to pay as a result of any such claims, actions, or lawsuits being

asserted against Licensor.

Licensor shall indemnify and defend Licensee against any loss or losses incurred through actions or lawsuits by third parties against Licensee for trade name, trademark, or service mark infringement, trademark or service mark dilution, unfair competition, and/or trade dress infringement arising out of Licensee's use of the Licensed Mark, and shall hold Licensee harmless for any damages, attorney fees, or other costs that Licensee may be required to pay as a result of any such claims, actions, or lawsuits being asserted against Licensee. In any such claim, action, or lawsuit brought by any third party against Licensee for trade name, trademark, or service mark infringement, trademark or service mark dilution, unfair competition, and/or trade dress infringement, Licensor shall assume and control the defense of the litigation and select and compensate counsel to defend the litigation.

8. INFRINGEMENT. Licensee shall promptly notify Licensor of any conflicting use or infringement of the Licensed Mark of which Licensee may become aware and shall cooperate with Licensor in every reasonable way to prosecute all acts or conduct that Licensor may deem necessary or advisable to protect the validity and exclusivity of Licensor's rights in the Licensed Mark. Licensee shall take no action independently of Licensor to prosecute any such acts or conduct without obtaining the prior, express, written approval of Licensor.

If Licensee brings to Licensor's attention an unauthorized third party use of the Licensed Mark, Licensor shall take steps to abate such use at Licensor's expense if Licensor, after investigation and evaluation of such unauthorized use, concludes that such use constitutes an infringement of its rights and that there is a reasonable probability of success in taking action to abate such infringement.

9. NOTICES. Any notice required or permitted under the terms of this Agreement must be given by registered letter, postage prepaid, addressed to the party to be notified at the address stated at the beginning of this Agreement, or at such other address as may be furnished in writing to the notifying party.

10. BINDING EFFECT. This Agreement shall be effective as of the date first above written and shall be binding upon and inure to the benefit of the parties hereto and their respective successors or assigns as permitted by this Agreement.

11. ENTIRE AGREEMENT. This Agreement constitutes the entire understanding between Licensor and Licensee regarding the subject matter hereof and may not be amended in any way except by an instrument in writing duly executed by both parties.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed in duplicate as of the date first above written.

Date: _ _ _ _ _ _

_ _[*NAME OF LICENSOR*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

Date: _ _ _ _ _ _

_ _[*NAME OF LICENSEE*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

© The Regents of the University of California

L. Assignments of Trademarks

§3.57 1. Generally

The Lanham Act provides that a registered mark (or a mark for which a registration application has been filed) is assignable by a duly executed written instrument along with the goodwill of the business in which the mark is used (or that the portion of the goodwill of the business associated with use of and symbolized by the mark). 15 USC §1060.

NOTE: Assignments of trademarks that are not accompanied by assignments of the core assets used to make the product or service that the trademark identifies (known as assignments "in gross") are invalid. A trademark assignment must include goodwill and the means to manufacture the trademarked goods or offer the trademarked services. "The purpose behind requiring that goodwill accompany the assigned mark is to maintain the continuity of the product or service symbolized by the mark and thereby avoid deceiving or confusing consumers." *E. & J. Gallo Winery v Gallo Cattle Co.* (9th Cir 1992) 967 F2d 1280, 1289.

Notarial acknowledgements are not required for validity, but constitute prima facie evidence of the execution of an assignment of a trademark. 15 USC §1060(a)(3). Title 15 USC §1060(a)(4) provides that an assignment is void against a subsequent purchaser for valuable consideration without notice, unless the prescribed information reporting the assignment has been recorded in the USPTO within three months after the date of the assignment or, in any event, before recordation of the later assignment. If recorded, the assignment must be accompanied by the USPTO's form of cover sheet for trademarks, a copy of which is reproduced in §3.59 and is available for downloading at http://www.uspto.gov/web/forms/pto1594.pdf. See 37 CFR §§3.1-3.41 for recording requirements.

There are special issues in connection with an assignment of a pending trademark application. An intent-to-use application may not be assigned before the applicant files an amendment to allege use under 15 USC §1051(d), unless the transfer is to a successor to the applicant's business (as in a merger or other sale of the company to third party) or to that portion of the business to which the mark pertains. 15 USC §1060; 37 CFR §3.16.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.58 2. Form: Trademark Assignment

§3.58 2. Form: Trademark Assignment

▶ To download **Word** version, right click and choose *Save Target As*

▶ To download **WordPerfect** version, right click and choose *Save Target As*

ASSIGNMENT OF TRADEMARK

This Assignment of Trademark is entered into as of _ _[*date*]_ _ **between** _ _[*name of assignor*]_ _, _ _[*address*]_ _ **("Assignor"), and** _ _[*name of assignee*]_ _, _ _[*address*]_ _ **("Assignee").**

Assignor has registered, is the sole owner of, and is using _ _[*name of mark*]_ _**, a mark registered in the United States Patent and Trademark Office, Registration No.** _ _[*number*]_ _**, dated** _ _[*date*]_ _ **and Assignee desires to acquire such mark.**

Therefore, in consideration of the payment of _ _[*dollar amount*]_ _**, receipt of which is acknowledged, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, Assignor does hereby assign to Assignee all rights, title, and interest in and to said mark, the goodwill of the business symbolized by said mark, along with the registration thereof, the number of which is contained herein.**

Date: _ _ _ _ _ _

_ _[*NAME OF ASSIGNOR*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.59 3. Form: U.S. Patent and Trademark Office Cover Sheet (Trademarks Only)

§3.59 3. Form: U.S. Patent and Trademark Office Cover Sheet (Trademarks Only)



Form **PTO-1594** (Rev. 01-09)
OMB Collection 0651-0027 (exp. 02/28/2009)

U.S. DEPARTMENT OF COMMERCE
United States Patent and Trademark Office

RECORDATION FORM COVER SHEET
TRADEMARKS ONLY

To the Director of the U. S. Patent and Trademark Office: Please record the attached documents or the new address(es) below.

1. Name of conveying party(ies):

☐ Individual(s) ☐ Association
☐ General Partnership ☐ Limited Partnership
☐ Corporation- State:_____
☐ Other_____

Citizenship (see guidelines)_____

Additional names of conveying parties attached? ☐ Yes ☐ No

2. Name and address of receiving party(ies)

Additional names, addresses, or citizenship attached? ☐ Yes ☐ No

Name:_____

Internal Address:_____

Street Address:_____

City:_____

State:_____

Country:_____ Zip:_____

☐ Association Citizenship _____
☐ General Partnership Citizenship _____
☐ Limited Partnership Citizenship _____
☐ Corporation Citizenship_____
☐ Other_____ Citizenship _____

If assignee is not domiciled in the United States, a domestic representative designation is attached: ☐ Yes ☐ No
(Designations must be a separate document from assignment)

3. Nature of conveyance)/Execution Date(s) :

Execution Date(s)_____

☐ Assignment ☐ Merger
☐ Security Agreement ☐ Change of Name
☐ Other_____

4. Application number(s) or registration number(s) and identification or description of the Trademark.

A. Trademark Application No.(s)

B. Trademark Registration No.(s)

Additional sheet(s) attached? ☐ Yes ☐ No

C. Identification or Description of Trademark(s) (and Filing Date if Application or Registration Number is unknown):

5. Name & address of party to whom correspondence concerning document should be mailed:

Name:_____

Internal Address:_____

Street Address: _____

City:_____

State:_____ Zip:_____

Phone Number: _____

Fax Number: _____

Email Address:_____

6. Total number of applications and registrations involved:

7. Total fee (37 CFR 2.6(b)(6) & 3.41) $_____

☐ Authorized to be charged to deposit account
☐ Enclosed

8. Payment Information:

Deposit Account Number _____

Authorized User Name _____

9. Signature:

_____ _____
Signature Date

_____
Name of Person Signing

Total number of pages including cover sheet, attachments, and document:

Documents to be recorded (including cover sheet) should be faxed to (571) 273-0140, or mailed to:
Mail Stop Assignment Recordation Services, Director of the USPTO, P.O. Box 1450, Alexandria, VA 22313-1450

Print

Guidelines for Completing Trademarks Cover Sheets (PTO-1594)

Cover Sheet information must be submitted with each document to be recorded. If the document to be recorded concerns both patents and trademarks, separate patent and trademark cover sheets, including any attached pages for continuing information, must accompany the document. All pages of the cover sheet should be numbered consecutively for example, if both a patent and trademark cover sheet is used, and information is continued on one additional page for both patents and trademarks, the pages of the cover sheet would be numbered from 1 to 4.

Item 1. Name of Conveying Party(ies).
Enter the full name of the party(ies) conveying the interest. If there is more than one conveying party, enter a check mark in the "Yes" box to indicate that additional information is attached. The name of the second and any subsequent conveying party(ies) should be placed on an attached page clearly identified as a continuation of the information in Item 1. Enter a check mark in the "No" box, if no information is contained on an attached page.

Item 2. Name and Address of Receiving Party(ies).
Enter the name and full address of the first party receiving the interest. If there is more than one party receiving the interest, enter a check mark in the "Yes" box to indicate that additional information is attached. If the receiving party is an individual, check the "other" box, place the word "individual" in the following line, and enter the citizenship of the receiving individual. If the receiving party is a legal entity, designate the legal entity of the receiving party by checking the appropriate box. If the receiving party has more than one citizenship, then the citizenship of **each** partner should be specified on an additional sheet, and "See additional sheet" should be written on the line for citizenship. A corporation must set forth the state, if applicable, or country of incorporation. An association must set forth the state, if applicable, or country under which they are organized. If the receiving party is not domiciled in the United States, a designation of domestic representative is encouraged. Place a check mark in the appropriate box to indicate whether or not a designation of domestic representative is attached. Enter a check mark in the "No" box if no information is contained on an attached page.

Item 3. Nature of Conveyance/Execution Date(s).
Enter the execution date(s) of the document. It is preferable to use the name of the month, or an abbreviation of that name, to minimize confusion over dates. In addition, place a check mark in the appropriate box describing the nature of the conveying document. If the "Other" box is checked, specify the nature of the conveyance. The "Other" box should be checked if the conveying/receiving party is correcting a previously filed document.

Item 4. Application Number(s) or Registration Number(s).
Indicate the application number(s) including series code and serial number, and/or registration number(s) against which the document is to be recorded. The identification of the trademark should be provided for all properties to avoid recordation against the wrong property. A filing date should be provided only when the application or registration number is unknown. Enter a check mark in the appropriate box: "Yes" or "No" if additional numbers appear on attached pages. Be sure to identify numbers included on attached pages as the continuation of Item 4.

Item 5. Name and Address of Party to whom correspondence concerning document should be mailed.
Enter the name and full address of the party to whom correspondence is to be mailed.

Item 6. Total Applications and Trademarks Involved.
Enter the total number of applications and trademarks identified for recordation. Be sure to include all applications and registrations identified on the cover sheet and on additional pages.

Block 7. Total Fee Enclosed.
Enter the total fee enclosed or authorized to be charged. A fee is required for each application and registration against which the document is recorded.

Item 8. Payment Information.
Enter the deposit account number and authorized user name to authorize charges.

Item 9. Signature.
Enter the name of the person submitting the document. The submitter must sign and date the cover sheet. Enter the total number of pages including the cover sheet, attachments, and document.

This collection of information is required by 35 USC 261 and 262 and 15 USC 1057 and 1060. The information is used by the public to submit (and by the USPTO to process) patent and trademark assignment requests. After the USPTO records the information, the records for patent and trademarks, assignments, and other associated documents can be inspected by the public. To view documents recorded under secrecy orders or documents recorded due to the interest of the federal government, a written authorization must be submitted. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the form to the USPTO. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Manager of the Assignment Division, Crystal Gateway 4, Room 310, 1213 Jefferson Davis Highway, Arlington, VA 22202. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop Assignment Recordation Services, Director of the USPTO, P.O. Box 1450, Alexandria, VA 22313-1450.

Print

Privacy Act Statement for Patent Assignment Recordation Form Cover Sheet

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with the above request for information. This collection of information is authorized by 35 U.S.C. 1, 2, 261 and E.O. 9424. This information will primarily be used by the USPTO for the recordation of assignments related to patents and patent applications. Submission of this information is voluntary but is required in order for the USPTO to record the requested assignment. If you do not provide the information required on the cover sheet, the assignment will not be recorded, and all documents will be returned to you.

After the information is recorded, the records and associated documents can be inspected by the public and are not confidential, except for documents that are sealed under secrecy orders or related to unpublished patent applications. Assignment records relating to unpublished patent applications are maintained in confidence in accordance with 35 U.S.C. 122. Records open to the public are searched by users for the purpose of determining ownership for other property rights with respect to patents and trademarks.

Routine uses of the information you provide may also include disclosure to appropriate Federal, state, local, or foreign agencies in support of their enforcement duties and statutory or regulatory missions, including investigating potential violations of law or contract and awarding contracts or other benefits; to a court, magistrate, or administrative tribunal in the course of presenting evidence; to members of Congress responding to requests for assistance from their constituents; to the Office of Management and Budget in connection with the review of private relief legislation; to the Department of Justice in connection with a Freedom of Information Act request; to a contractor in the performance of their duties; to the Office of Personnel Management for personnel studies; and to the General Services Administration (GSA) as part of their records management responsibilities under the authority of 44 U.S.C. 2904 and 2906. Such disclosure to GSA shall not be used to make determinations about individuals.

© The Regents of the University of California

M. Violations of Trademark Rights

§3.60 1. Trademark Infringement

A claim of infringement of a federally registered trademark must be brought in federal court. 15 USC §1121. A plaintiff asserting an infringement claim under the Lanham Act must show that the plaintiff owns a federally registered mark and that the defendant's use of the mark in commerce without the plaintiff's consent creates a likelihood of confusion, mistake, or deception as to the origin of the defendant's product or service. See 15 USC §1114. See generally California Business Litigation, chap 6 (Cal CEB 2002). The Ninth Circuit employs an eight-factor test to determine whether a likelihood of confusion exists (*Playboy Enters. v Netscape Communications Corp.* (9th Cir 2004) 354 F3d 1020, 1026):

- The strength of the mark;
- The proximity of the goods;
- The similarity of the marks;
- Any evidence of actual confusion;
- The marketing channels used;
- The type of goods and the degree of care likely to be exercised by the purchaser;
- The defendant's intent in selecting the mark; and
- The likelihood of expansion of the product lines.

See also *AMF Inc. v Sleekcraft Boats* (9th Cir 1979) 599 F2d 341. Some factors, such as evidence of actual confusion and similarity of the marks, are more important than others. However, one factor alone will generally not be dispositive, and courts must consider the factors "that are of the most relative importance" in the case. *Jada Toys, Inc. v Mattel, Inc.* (9th Cir 2008) 518 F3d 628, 632. In Internet cases, some factors may not even apply. In *Playboy Enterprises, supra,* the Ninth Circuit admonished courts to be flexible in applying them in the context of the Internet. 354 F2d at 1026.

Sellers of goods on the Internet should be aware of potential liability for contributory trademark infringement. Contributory infringement has been defined by the U.S. Supreme Court as follows (*Inwood Labs., Inc. v Ives Labs., Inc.* (1982) 456 US 844, 854, 72 L Ed 2d 606, 615, 102 S Ct 2182):

> [I]f a manufacturer or distributor intentionally induces another to infringe a trademark, or if it continues to supply its product to one whom it knows or has reason to know is engaging in trademark infringement, the manufacturer or distributor is contributorially responsible for any harm done as a result of the deceit.

Although *Inwood* expressly refers only to manufacturers and distributors of products, the case has been read to impose liability for contributory trademark infringement more broadly and has been applied, for example, in the context of website operators and service providers. See *Perfect 10, Inc. v Visa Int'l Serv. Ass'n* (9th Cir 2007) 494 F3d 788, 807, cert denied (2008) ___ US ___, 171 L Ed 2d 811, 128 S Ct 2871; *Lockheed Martin Corp. v Network Solutions, Inc.* (9th Cir 1999) 194 F3d 980, 984.

In *Tiffany Inc. v eBay, Inc.* (SD NY 2008) 576 F Supp 2d 463, Tiffany attempted to hold eBay liable for contributory infringement for permitting counterfeit Tiffany jewelry to be sold by eBay members on eBay's auction website. Applying the *Inwood* test, the court held that eBay could not be held liable "based solely on their generalized knowledge that trademark infringement might be occurring on their websites." 576 F Supp 2d at 527. The court noted actions eBay took in response to notice of infringing items, including warning and suspending sellers and adopting measures to prevent and identify fraud. The court found that eBay was "not willfully blind to infringement"; when it had knowledge of specific infringing auction listings, it promptly terminated those listings. 576 F Supp 2d at 518. Further, the court noted that, when eBay had knowledge that a seller was repeatedly engaging in counterfeit activity, eBay's pattern was to suspend that seller and then take further corrective action.

But see *Louis Vuitton Malletier, S.A. v Akanoc Solutions, Inc.* (ND Cal 2008) 591 F Supp 2d 1098, in which a federal

jury in California awarded $32 million in damages in a case involving contributory infringement. The jury found two Internet service providers (ISPs) liable because they hosted websites selling counterfeit Louis Vuitton goods. Louis Vuitton was able to demonstrate the ISPs were aware of the infringing websites and did not take them down. See http://www.scribd.com/doc/19283259/Louis-Vuitton-v-Akanoc-Jury-Verdict.

© The Regents of the University of California

§3.61 2. False Designation or Description

The Lanham Act also allows a claim to be brought for false designation of origin, false description, or false or misleading representation of fact in connection with goods or services in commerce, regardless of whether the plaintiff's mark is registered or unregistered. Under 15 USC §1125(a):

> Any person who, on or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol, or device, or combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact which—
>
> (A) is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person, or
>
> (B) in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities, shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act.

Examples of unfair trade practices include "palming off" and "reverse palming off." Palming off occurs when a mark is used on products or services not authorized by the mark owner, and the defendant unfairly reaps the benefits of the significance of the mark. See *Echo Travel, Inc. v Travel Assocs., Inc.* (1989) 870 F2d 1264. Reverse palming off occurs when a mark on a product is removed and replaced with an entirely different mark. *Faulkner v National Geographic Soc'y* (SD NY 2002) 211 F Supp 2d 450.

Penal Code §350 sets forth penalties for use of a counterfeit registered trademark. An individual or business entity convicted of using a counterfeit mark is required to pay restitution to the trademark owner. Pen C §350(i).

© The Regents of the University of California

§3.62 3. ACPA

The Anticybersquatting Consumer Protection Act (ACPA) (15 USC §1125(d)), which is now part of the Lanham Act, also provides protection for owners of marks. For further discussion of the ACPA, see §§3.22-3.25.

© The Regents of the University of California

§3.63 4. Remedies for Trademark Infringement

An injunction may be obtained under 15 USC §1116 by showing irreparable injury and likelihood of success on the merits. Under 15 USC §1117(a), damages may also be sought for trademark infringement, false designations of origin, false description, dilution of famous marks, and cybersquatting, as discussed in §§3.60-3.68. The plaintiff may recover the defendant's profits, any damages sustained by the plaintiff, and the cost of the litigation, including reasonable attorney fees in exceptional cases. The court may increase or decrease the damages award if the court finds that the amount of recovery based on profits is inadequate or excessive. 15 USC §1117(a). Damages are generally awarded to compensate the owner and not to penalize the defendant. If the case relates to cyberpiracy under the Anticybersquatting Consumer Protection Act (ACPA), the plaintiff may elect not to recover actual damages and profits, and receive an award of statutory damages between $1000 to $100,000 per domain name infringement.

Some plaintiff trademark owners have asked the court to order the transfer of infringing domain names to the mark owners. Although the court has discretion to order domain name transfers, the plaintiff must first prove cybersquatting as defined by the ACPA. *Interstellar Starship Servs., Ltd. v EPIX, Inc.* (9th Cir 2002) 304 F3d 936, 948. For further discussion of ACPA actions, see §§3.22-3.25.

California's Anti-Phishing Act of 2005 (Bus & P C §§22948-22948.3), effective January 1, 2006, makes it unlawful for an entity or an individual to use the Internet, including e-mail, to "induce another person to provide identifying information by representing itself to be a business without the authority or approval of the business." Bus & P C §22948.2. Adversely affected owners of websites and trademarks are eligible for the greater of actual damages or $500,000. Bus & P C §22948.3(a)(1).

© The Regents of the University of California

§3.64 5. Defenses to Trademark Infringement

Defenses to an infringement claim may include the following (see *Moore Bus. Forms v Ryu* (5th Cir 1992) 960 F2d 486):

- There is no likelihood of confusion between the marks because there are differences between the marks, or the goods or services associated with the marks are different;
- Laches or estoppel if the mark owner has not enforced its rights; and
- The mark is considered abandoned (*e.g.,* the mark owner licensed its trademark in an unrestricted manner).

Other potential defenses include fair use, nominative use, and functional use. See generally *Playboy Enters. v Netscape Communications Corp.* (9th Cir 2004) 354 F3d 1020, 1029. The defense of nominative use is discussed in §3.72.

Trademark fair use provides an alleged infringer with a statutory defense when (15 USC §1115(b)(4)):

> the use of the name, term, or device charged to be an infringement is a use, otherwise than as a mark… of a term or device which is descriptive of and used fairly and in good faith only to describe the goods or services of such party, or their geographic origin.

Until recently, federal appellate courts were divided on whether likelihood of confusion bars this defense (the view of the Fifth, Sixth, and Ninth Circuits) or whether no such bar exists (the view of the Second, Fourth, and Seventh Circuits). In *KP Permanent Make-Up, Inc. v Lasting Impression, Inc.* (2004) 543 US 111, 160 L Ed 2d 440, 125 S Ct 542, the U.S. Supreme Court resolved the split, holding that likelihood of confusion is no bar to the statutory fair use defense. In *Lasting Impression,* both parties sold permanent makeup to be injected under the skin. Plaintiff owned a trademark for the term "Micro Colors." Defendant used the same term on advertising material and pigment bottles. Plaintiff sued, alleging that defendant was infringing its trademark. The district court found that defendant used the term fairly and in good faith, only to describe its goods and not as a mark. In reaching its decision, the court did not examine whether defendant's use of "microcolor" was likely to cause confusion. The Supreme Court upheld this approach, noting that "it is only when a plaintiff has shown likely confusion by a preponderance of the evidence that a defendant could have any need for an affirmative defense." 160 L Ed 2d at 450. Thus, to have any relevance at all, the fair use defense would have to be available despite a likelihood of confusion. The Court stated, however, that its holding did not foreclose the relevance of the extent of any likelihood of confusion in assessing whether a defendant's use was objectively fair. Thus, a defendant arguing for fair use may still have to show that any likelihood of confusion is not significant.

A defense to trademark infringement may be available to operators of "gripe" sites that are noncommercial in nature and are merely critical of a trademark owner's goods or services. In *Bosley Med. Inst. v Kremer* (9th Cir 2005) 403 F3d 672, the court held that noncommercial use of a trademark as the domain name of a website where the subject is consumer commentary about the products and services represented by the mark does not constitute infringement under the Lanham Act. The court found in favor of the defendant, whose gripe site at http://www.bosleymedical.com used the trademark of his target in the domain name. On the critical question of whether the griper was using the domain name in commerce, the court found that the site generated no revenues and did not promote any goods or services. It did link to another website, which through a series of further links could lead to commercial advertisements. It would be ridiculous to collapse this chain of links into a conclusion that the domain name use was commercial, and the Ninth Circuit wisely rejected that illogic ("[t]his roundabout path to the advertising of others is too attenuated to render Kremer's site commercial"). 403 F3d at 678.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.65 6. Dilution of Famous Mark

§3.65 6. Dilution of Famous Mark

The Federal Trademark Dilution Act of 1995 (15 USC §1125) (the FTDA, also known as the Anti-Dilution Act) was enacted to protect registered and unregistered famous trademarks, service marks, and trade dress from dilution. *Nissan Motor Co. v Nissan Computer Corp.* (9th Cir 2004) 378 F3d 1002, 1011. The Trademark Dilution Revision Act of 2006 (TDRA) (Pub L 109-312, 120 Stat 1730) expands and revises the FTDA to protect famous trademarks from uses that blur the distinctiveness of the mark

In *Moseley v V Secret Catalogue, Inc.* (2003) 537 US 418, 155 L Ed 2d 1, 123 S Ct 1115, the United States Supreme Court held that the FTDA required a showing of "actual dilution," not merely the likelihood of harm, for a plaintiff to succeed in a dilution claim under the FTDA. In the aftermath of the *Moseley* case, substantial questions remained regarding how a plaintiff might prove actual dilution, such as whether a plaintiff had to establish economic loss.

The Trademark Dilution Revision Act of 2006 (TDRA) overruled the Supreme Court's holding in *Moseley* that a dilution plaintiff must prove "actual" dilution. As amended, 15 USC §1125(c) states that the owner of a famous mark is entitled to enjoin use of a mark or trade name "that is likely to cause dilution by blurring or dilution by tarnishment of the famous mark, regardless of the presence or absence of actual or likely confusion, of competition, or of actual economic injury." 15 USC §1125(c)(1). A plaintiff claiming dilution no longer bears the evidentiary burden of proving actual dilution, and as the owner of a famous mark may obtain relief before harm is done to the value of its famous mark.

The TDRA affords protection from dilution not only to famous marks that are inherently distinctive, but also to those that have achieved secondary meaning. Section 1125(c) protects famous marks that are "distinctive, inherently or through acquired distinctiveness." 15 USC §1125(c)(1). This language resolves a split in the Circuits as to whether a mark that is famous but not inherently distinctive is entitled to protection from dilution. Compare, *e.g.,* holdings in *Times Mirror Magazines Inc. v Las Vegas Sports News* (3d Cir 2000) 212 F3d 157, 167 ("we are not persuaded that a mark be subject to separate tests for fame and [acquired] distinctive[ness]" with *Savin Corp. v Savin Group* (2d Cir 2004) 391 F3d 439, 449 ("In this Circuit, to sustain a claim under the FTDA … a plaintiff must show that the senior mark possesses both a 'significant degree of inherent distinctiveness' and fame").

As revised, §1125(c)(2) describes two categories of dilution not specifically named in the FTDA: dilution by "blurring" and by "tarnishment." Dilution by blurring is defined as an association arising from the similarity between a famous mark and diluting mark "that impairs the distinctiveness of the famous mark." Section 1125(c)(2)(B) articulates six nonexclusive factors a court may consider in determining whether a mark is likely to cause dilution by blurring:

> (i) the degree of similarity between the diluting mark and the famous mark;
> (ii) the degree of distinctiveness of the famous mark;
> (iii) the extent to which the owner of the famous mark is engaged in "substantially exclusive use of the mark";
> (iv) the degree of recognition of the famous mark;
> (v) whether the user of the diluting mark intended to create an association between it and the famous mark; and
> (vi) any actual association between the diluting mark and the famous mark.

Prior case law also acknowledges blurring as a means of dilution and describes blurring as a gradual whittling away of a mark's selling power and distinctiveness through its unauthorized use by others on dissimilar products. *Mead Data Cent. v Toyota Motor Sales USA, Inc.* (2d Cir 1989) 875 F2d 1026, 1031; *Mattel, Inc. v MCA Records Inc.* (9th Cir 2002) 296 F3d 894, 908, cert denied (2003) 537 US 1171. A key question in analysis of a potential blurring claim is whether the marks are similar enough to give rise to dilution. Courts have held that the mark used by the alleged diluter must be identical, or nearly identical, to the protected mark for a dilution claim to succeed. *Nissan Motor Co. v Nissan Computer Corp.* (9th Cir 2004) 378 F3d 1002, 1011. The Ninth Circuit has held that the similarity requirement is less stringent in circumstances where the senior mark is highly distinctive and the junior mark is used for a closely related product. *PerfumeBay.com, Inc v Ebay, Inc.* (9th Cir 2007) 506 F3d 1165. In *PerfumeBay*, the court found that PerfumeBay marks contained the dominant suffix "Bay" to sell products also offered by eBay and concluded that

consumers might no longer associate the usage of the "Bay" suffix with eBay's services, *i.e*., the sale of products on an Internet-based marketplace. 506 F3d at 1181.

Section 1125(c)(2)(C) defines "dilution by tarnishment" as an association arising from the similarity between a famous mark and diluting mark "that harms the reputation of the famous mark." The TDRA, however, does not provide a set of factors to assess the likelihood of tarnishment. Prior case law may provide insight into the factors to be used. The court in *Hormel Foods Corp. v Jim Henson Prods., Inc*. (2d Cir 1996) 73 F3d 497, 506, held that tarnishment occurs when a mark is improperly associated with an inferior or offensive product or service. In *Toys R Us, Inc. v Akkaoui* (ND Cal, Oct. 29, 1996, No. C 96-3381) 1996 US Dist Lexis 17090, the owner of Toys R Us sued the defendant for using "adultsrus.com" as a domain name and Adults R Us as a mark for operating a pornography website. Finding that the defendant's use of Adults R Us was likely to tarnish the plaintiff's marks by associating them with pornography, the court enjoined the defendant from operating any website containing "R Us." See also *Ford Motor Co. v Lapertosa* (ED Mich 2001) 126 F Supp 2d 463, 468.

© The Regents of the University of California

§3.66 a. Factors Bearing on Whether Mark Is Famous

The TDRA defines a "famous" mark as one that "is widely recognized by the general consuming public of the United States as a designation of source of the goods or services." 15 USC §1125(c)(2). This definition is intended to eliminate the concept of "niche" fame, recognized in some cases as existing among a small group of purchasers or in a limited geographic area. The TDRA provides the following four factors that courts may use, among others, in determining whether a mark is famous (15 USC §1125(c)(2)(A):

- The duration, extent, and geographic reach of advertising and publicity of the mark;
- The amount, volume, and geographic extent of sales under the mark;
- The extent of actual recognition of the mark; and
- Whether the mark is registered.

Although there is currently no case law interpreting the TDRA factors, an example of a mark found to be famous under prior law is the "Barbie" mark owned by Mattel. The court in *Mattel, Inc. v Internet Dimension, Inc.* (SD NY, July 13, 2000, No. 99 CIV 10066) 2000 US Dist Lexis 9747 held that, while the name "Barbie" was not inherently distinctive, it had gained distinctiveness through four decades of Mattel's marketing and sales of Barbie dolls to the public. The court ruled in Mattel's favor, holding that the degree of distinctiveness of the mark "Barbie" was great, because Mattel had continuously used the mark to sell the product. The court noted that Mattel had spent millions of dollars on advertising its product and had sold Barbie dolls and other Barbie products in various retail chains across the nation and on the company's website (which was accessible around the world). The court further noted that Mattel had always challenged those who infringed upon its mark, and that the "Barbie" trademark was registered with the United States Patent and Trademark Office.

© The Regents of the University of California

§3.67 b. Cybersquatting and Dilution

To be actionable, the Anti-Dilution Act requires that an infringing mark or domain name be used "in commerce." 15 USC §1125(a)(1). In the cybersquatting context, a plaintiff may have difficulty proving that an infringing domain name is used in commerce. A cybersquatter typically purchases a domain name with the name of a famous mark in hopes of selling it to the owner of the famous mark. Some cyber-squatters have argued that domain name registration is not a commercial use of the mark, because cybersquatters do not usually advertise or sell the domain name. Courts have held that purchasing domain names for the purpose of selling them to their owners is a commercial use of the mark, and thus is sufficient to prove an anti-dilution claim. *Bird v Parsons* (6th Cir 2002) 289 F3d 865.

© The Regents of the University of California

§3.68 7. Remedies and Defenses to Anti-Dilution Claims

Under the TDRA, a party found to have used a mark likely to cause dilution can be enjoined and, in addition, may be held liable to the owner of the famous mark for profits, damages, and costs if the infringing party "willfully intended to trade on the recognition of the famous mark," or "willfully intended to harm the reputation of the famous mark." 15 USC §1125(c)(5)(B)(ii).

There are a number of defenses to a claim of dilution. Section 1125 provides that the following are not actionable as dilution (15 USC §1125(c)(3)(A)):

> (A) Any fair use, including a nominative or descriptive fair use, or facilitation of such fair use, of a famous mark by another person other than as a designation of source for the person's own goods or services, including use in connection with—
> (i) advertising or promotion that permits consumers to compare goods or services; or
> (ii) identifying and parodying, criticizing, or commenting upon the famous mark owner or the goods or services of the famous mark owner.
> (B) All forms of news reporting and news commentary.
> (C) Any noncommercial use of a mark.

The fair use doctrine allows uses of a mark in good faith if the mark is used only to describe the goods or services of a party or the geographic origin of the goods or services. *Brother Records, Inc. v Jardine* (9th Cir 2003) 318 F3d 900, cert denied (2003) 540 US 824. For example, in *Volkswagenwerk Aktiengesellschaft v Church* (9th Cir 1969) 411 F2d 350, 352, the Ninth Circuit explained that, although use of the name "Modern Volkswagen Porsche Service" was unlawful, when the defendant used the name "Volkswagen" in addition to the word "Independent," it effectively put consumers on notice that the defendant was not affiliated with Volkswagen, rendering such use permissible. The court stated that the defendant could advertise that he repaired Volkswagen cars, but could not do so in a manner that would likely suggest to customers that he was affiliated with Volkswagen A.G. For a more recent case in which the fair use defense was asserted, see *Horphag Research Ltd. v Pellegrini* (9th Cir 2003) 337 F3d 1036, cert denied (2004) 540 US 1111. See also the discussion of nominative fair use in §3.72.

© The Regents of the University of California

8. Sample Cease and Desist Letter

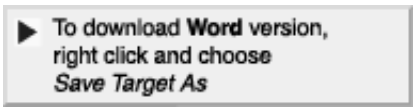
§3.69 a. Introduction

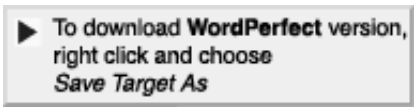
In an effort to avoid litigation, the owner of a mark should attempt to stop an infringer from violating the owner's intellectual property rights by sending a cease and desist letter. The letter explains that the mark is protected and that it is being used in a manner that conflicts with the rights of the mark owner, and requests the person to whom it is addressed to cease all uses of the mark.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.70 b. Form: Sample Cease and Desist Letter

§3.70 b. Form: Sample Cease and Desist Letter





[*Attorney's letterhead*]

_ _[*Date*]_ _

_ _[*Name and address*]_ _

Re: _ _[*Name of infringing website*]_ _

This firm represents _ _[*name of client*]_ _ in various matters relating to intellectual property.

Our client has been continuously using the mark _ _[*name of mark*]_ _ in connection with its business and on web pages at least as early as _ _[*date*]_ _. Consequently, _ _[*name of mark*]_ _ represents an extremely valuable trademark of our client that must be protected from potential marketplace confusion.

[*Add one of the following alternatives*]

[*Alternative 1: Use if trademark registration is pending*]

Moreover, our client has filed an application for federal trademark registration for the mark in _ _[*date*]_ _ of this year.

[*Alternative 2: Use if mark is federally registered*]

Moreover, our client has a registration certificate evidencing that its mark is federally registered.

[*Continue*]

It has recently come to our client's attention that your website at _ _[*URL of infringing website*]_ _ uses the _ _[*name of mark*]_ _ mark. Such usage may create a likelihood of confusion with our client's _ _[*name of mark*]_ _ mark that could lead consumers to the mistaken belief that you, your company, and/or your website is affiliated with, sponsored by, or endorsed by our client. Therefore, your use of the mark constitutes infringement under the United States trademark laws.

As a result, we request that you discontinue use of the term _ _[*name of mark*]_ _ on your website and elsewhere.

[*If appropriate, add*]

or, alternatively, at a minimum, indicate in connection with all uses of the term that the _ _[*name of mark*]_ _ mark is a trademark of our client and that neither you nor your company are affiliated with, endorsed by, or sponsored by our client. Additionally, if you choose the latter option, we require that you include a prominent link (which meets with our client's approval) to our client's website, _ _[*name of client's website*]_ _, on the main page of your site.

[*Continue*]

Given the importance of this issue to our client, we would like to receive either your or your counsel's letter within 10 business days confirming how you will comply with our request.

We thank you in advance for your cooperation in resolving this matter without the necessity for legal action.

Yours truly,

Date: _ _ _ _ _ _ _ _[*Name of firm*]_ _

By: __[*Signature*]__
_ _[*Typed name*]_ _

© The Regents of the University of California

III. METATAGS AND SEARCH TERMS

§3.71 A. Introduction

A website may be found either by typing the website address, if known, in the address bar in the Internet browser or by submitting a keyword query to a search engine. Search engines locate and provide a list of hyperlinks to websites matching the user's keyword query. In order to respond quickly and accurately to the query, most search engines use "spider" or "crawler" software to collect and index addresses of pertinent websites. Website owners or operators may increase the likelihood that their site will be retrieved by spiders or crawlers by using metatags. Metatags are text of HTML coding that are hidden from normal view, but are visible if the website's source code is retrieved. Trademark law is implicated when metatags use trademarks owned by third parties. Following is an example of a source code containing metatags that incorporate third party trademarks; use of these metatags led to allegations of trademark infringement in *Playboy Enters., Inc. v Welles* (9th Cir 2002) 279 F3d 796:

<html>

<head><title>Terri Welles Erotica</title>

<META NAME= "description" CONTENT= "Playboy Playmate of the Year 1981 Terri Welles website featuring erotic nude photos, semi-nude photos, softcore and exclusive Members Club">

<META NAME= "keywords" CONTENT= "terri, welles, playmate, playboy, model, models, nude, naked…"

The higher up a website appears in a search retrieval list, the greater the likelihood it will be found and accessed by a user. To increase the likelihood of a website's hyperlink appearing near the top of the search result list, an operator can either pay the search engine for priority placement on the search result list, or use methods such as keyword metatags in the website's HTML code. Search engines usually rank sites by relevance, and some search engines determine a site's relevance, in part, by the number of times a given search term appears on a website's page or source code. Frequent use of a metatag in the HTML code may increase the likelihood of the website's hyperlink appearing prominently on the search results page. Certain Internet search engines also accept payment for "sponsored links" by which a website can pay for its link to appear in a special section if certain search terms are used. An example is Google's AdWords program, described in more detail at http://adwords.google.com. For further discussion of search engine optimization, see §§17.29A-17.29B.

As use of the Internet has expanded, the sophistication of search engine ranking methodology has also increased, so that many search engines use complex algorithms that do not rely on reference to embedded html code in order to conduct rankings. Although the significance of metatags in ranking methodology has decreased over time, many Internet companies still use them, and care should be taken not to run afoul of trademark law. Using a trademark of another person or entity as a metatag may violate the Lanham Act (15 USC §§1051-1141n). Although metatags are normally invisible to Internet users, courts have applied the "likelihood of confusion" test of the Lanham Act (see 15 USC §1114(1)) to the use of third party trademarks as metatags. Sections 3.72-3.76 explore when use of third party trademarks is acceptable and issues to consider before using a third party trademark in a metatag.

PRACTICE TIP: When reviewing a website to determine whether licenses or releases should be obtained from third parties for use of intellectual property on the site (see generally chap 14), counsel should also consider any use of third party trademarks as metatags in the website's HTML code as a possible source of trademark infringement.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.72 B. Nominative Fair Use

§3.72 B. Nominative Fair Use

"Nominative fair use" is a defense to allegations of trademark infringement for defendants whose use of a another party's trademark "does not attempt to capitalize on consumer confusion or to appropriate the cachet of one product for a different one." *New Kids on the Block v News Am. Publ'g, Inc*. (9th Cir 1992) 971 F2d 302, 307. See also *Playboy Enters. v Netscape Communications Corp.* (9th Cir 2004) 354 F3d 1020, 1029; *Horphag Research Ltd. v Pellegrini* (9th Cir 2003) 337 F3d 1036, 1041, cert denied (2004) 540 US 1111. In the *New Kids* case, the two newspaper defendants had conducted reader polls asking which of the New Kids on the Block was the most famous. The Ninth Circuit established a three-factor test to determine whether a commercial user is entitled to a nominative fair use defense in cases where the defendant uses the plaintiff's trademark to describe the plaintiff's product, rather than its own (*New Kids on the Block,* 971 F2d at 308):

- First, the product or service in question must be one not readily identifiable without use of the trademark;
- Second, only so much of the mark or marks may be used as is reasonably necessary to identify the product or service; and
- Third, the user must do nothing that would, in conjunction with the mark, suggest sponsorship or endorsement by the trademark holder.

In *Playboy Enters. v Netscape Communications Corp.* (9th Cir 2004) 354 F3d 1020, 1029, the defendants were using the words "playboy" and "playmate," along with about 400 others, as key words to link adult-oriented banner advertising with particular search results. The Ninth Circuit held that defendants were not entitled to the nominative use defense, because their use of the plaintiff's marks was not absolutely required to trigger the adult-oriented advertisements.

In *Playboy Enters., Inc. v Welles* (9th Cir 2002) 279 F3d 796, 801, the court found the defendant was entitled to the nominative use defense because, as a former Playboy Bunny, she would be unable to describe herself on her website without utilizing plaintiff Playboy Enterprises' trademarks in her metatags. 279 F3d at 802. The court found the defendant used the trademarks in her metatags only to the extent necessary and avoided repeated use that would have ranked her website at or near the top of a search retrieval list. The court also found that the defendant did "nothing in conjunction with her use of *[the trademarks]* to suggest sponsorship or endorsement by *[the trademark holder]*." 279 F3d at 803. This was supported by the fact that on her website the defendant expressly disclaimed sponsorship by the plaintiff.

By employing the three-factor test set forth in *New Kids on the Block v News Am. Publ'g, Inc., supra*, the *Welles* court rejected for nominative use cases the eight-factor *Sleekcraft* test (*AMF Inc. v Sleekcraft Boats* (9th Cir 1979) 599 F2d 341) traditionally used in trademark infringement cases to determine whether a likelihood of confusion exists. *Playboy Enters., Inc.,* 279 F3d at 801. See also *Brookfield Communications, Inc. v West Coast Entertainment Corp*. (9th Cir 1999) 174 F3d 1036, 1053, in which the court stated: "We must be acutely aware of excessive rigidity when applying the law in the Internet context; emerging technologies require a flexible approach." 174 F3d at 1054. See also *Tiffany Inc. v eBay, Inc.* (SD NY 2008) 576 F Supp 2d 463 (eBay's use of Tiffany's marks protected as nominative fair use because Tiffany jewelry sold on eBay's site was not readily identifiable without use of Tiffany trademark and no sponsorship or endorsement was implied).

PRACTICE TIPS: If an online business's use of a third party trademark is nominative, an appropriate disclaimer should be added to its website. The *Welles* disclaimer stated the following: "This site is neither endorsed, nor sponsored, nor affiliated with Playboy Enterprises, Inc. Playboy® Playmate of the Year® and Playmate of the Month® are registered trademarks of Playboy Enterprises, Inc." 279 F3d at 799 n1. Online businesses should also be counseled not to use a third party's trademark as a metatag to improve the website's ranking in search results. Further, third party trademarks should be used as few times as possible in the HTML source code, because the frequency of use of the third party's trademark can negate a finding of nominative fair use. If an online business intends to use a third party trademark in a way that may not qualify for the nominative use defense, other potential

exceptions to the Lanham Act (news reporting and news commentary, noncommercial uses, or fair uses of the trademark) should be considered. These exceptions are more fully discussed in §§3.64-3.68.

© The Regents of the University of California

§3.73 C. Initial Interest Confusion Test

Trademark infringement issues also arise if there are strong similarities between third party trademarks and words used as metatags or in other Internet search-related contexts. Courts have applied the so-called "initial interest confusion" test (see *Dr. Seuss Enters., L.P. v Penguin Books USA, Inc.* (9th Cir 1997) 109 F3d 1394, 1405, cert dismissed (1997) 521 US 1146) to evaluate whether metatags are infringing.

Use of competitor's mark as metatag. Even if no actual sale is completed as a result of the confusion, a mark may be deemed confusingly similar if it is used to capture the initial attention of a consumer. *Brookfield Communications, Inc. v West Coast Entertainment Corp*. (9th Cir 1999) 174 F3d 1036, 1062. In the *Brookfield* case, the Ninth Circuit found that the defendant's use of the term "movie buff" in metatags led users looking for plaintiff's "MovieBuff" products to the defendant's "westcoastvideo.com," which offered products similar to those sold on the plaintiff's website. The defendant's acts thus created a likelihood of confusion, and the court granted the plaintiff's request for a preliminary injunction. See also *North Am. Med. Corp. v Axiom Worldwide, Inc.* (11th Cir 2008) 522 F3d 1211 (use of competitor's trademarks as metatags held to be "use in commerce" and actionable under Lanham Act); *Venture Tape Corp. v McGills Glass Warehouse* (1st Cir 2008) 540 F3d 56 (use of competitor's trademarks as metatags created likelihood of confusion and resulted in award of $426,487 in damages, costs, and attorney fees); *Deltek, Inc. v Iuvo Sys., Inc.* (ED Va, Apr. 20, 2009, No. 1:09cv330) 2009 US Dist Lexis 33555, *24 (use of competitor's trademarks as metatags may cause consumer to believe an affiliation between the two entities exists and may constitute improper "attempt to trade on the commercial value associated with the marks"). But see *Designer Skin, LLC v S&L Vitamins, Inc.* (D Ariz 2008) 560 F Supp 2d 811 (use of manufacturer's trademarks in metatags and key words did not result in initial interest confusion when defendant reseller actually sold manufacturer's goods and use of marks accurately described goods for sale on defendant's site); *Standard Process, Inc. v Banks* (ED Wis 2008) 554 F Supp 2d 866 (rejecting initial interest confusion argument, in part because of decreased relevance of metatags in search engine methodology and because defendant was reseller of plaintiff's goods).

Keying. Another case supporting the applicability of the Lanham Act to the use of a competitor's marks on the Internet is *Playboy Enters. v Netscape Communications Corp.* (9th Cir 2004) 354 F3d 1020. The *Playboy* case involved the practice of "keying," in which the operators of search engines, for a fee, display an advertiser's ad on a search results page when a consumer types a designated term into the operator's search engine. In this case, the "keyed" terms included plaintiff's trademarks and tied the display of Netscape's clients' adult-oriented ads to plaintiff's marks. The Ninth Circuit held that when the advertiser's banner ad is not labeled so as to identify its source, this practice could result in trademark infringement by application of the "initial interest confusion" doctrine.

Sponsored links tied to competitor's mark. Offering sponsored links tied to searches of competitor's marks has been held to constitute trademark infringement. In *Government Employees Ins. Co. v Google, Inc.* (ED Va 2004) 330 F Supp 2d 700, a "sponsored link" resulted in placement in Internet search results based on the search engine's use of a trademark. The court held that the sale to other companies of the ability to link their websites to Google search results for the term "GEICO" constituted use of the trademark in commerce. 330 F Supp 2d at 704.

No "internal use" defense. Defendants have argued that the sale of trademarks as keywords for sponsored links does not constitute "use" within the meaning of the Lanham Act because such a use is for internal purposes, not visible to the public and, therefore, should not be actionable. This "internal use" argument was rejected in *Rescuecom Corp. v Google, Inc.* (2d Cir 2009) 562 F3d 123. The Second Circuit ruled that using a competitor's trademarks as a trigger for search-related advertising is a "use in commerce" within the meaning of the Lanham Act and is, therefore, actionable. The court explained that this result is necessary in order to comply with the intention of the Lanham Act "to make actionable the deceptive and misleading use of marks in commerce." 562 F3d at 138. Otherwise, alleging an "internal use" would effectively insulate an alleged infringer from a charge of infringement, no matter how likely the use is to cause confusion in the marketplace. 562 F3d at 130.

A Pennsylvania court considering the sale of trademarks in Google's AdWords program also rejected the "internal use" arguments, concluding that "[b]y establishing an opportunity to reach consumers via alleged purchase and/or use

of a protected trademark, defendant has crossed the line from internal use to use in commerce under the Lanham Act." *J.G. Wentworth, S.S.C. LP v Settlement Funding LLC* (ED Pa, Jan. 4, 2007, No. 06-0597) 2007 US Dist Lexis 288, *17. See also *Boston Duck Tours, LP v Super Duck Tours, LLC* (D Mass 2007) 527 F Supp 2d 205, rev'd on other grounds (1st Cir 2008) 531 F3d 1 (purchase of sponsored links triggered by search conducted on competitor's name constitutes use in commerce actionable under trademark law; however, no Lanham Act violation occurred because mark defendant used in ads triggered by links (Super Duck Excursions) not likely to infringe plaintiff's mark (Boston Duck Tours)). But see *Storus Corp. v Aroa Mktg., Inc.* (ND Cal 2008) 87 USPQ2D 1032 (initial interest confusion found when, on 1374 occasions, consumers searching plaintiff's website by using plaintiff's mark were "diverted" to defendant's website offering competing product).

At least one court in the Ninth Circuit has also rejected the "internal use" defense, holding that the sale of trademarked terms in Google's AdWords program is a use in commerce for purposes of the Lanham Act. Under the AdWords program, Google sold online advertising triggered by a search for American Blind's trademark and displayed advertising belonging to American Blind's competitors. *Google Inc. v American Blind & Wallpaper Factory, Inc.* (ND Cal, Apr. 18, 2007, No. C03-5340 JF (RS)) 2007 US Dist Lexis 32450.

© The Regents of the University of California

§3.74 D. Protection of Fanciful Marks

Fanciful marks, "purely the product of imagination *[with]* no logical association with the product," receive strong protection from the courts. *Eli Lilly & Co. v Natural Answers Inc.* (7th Cir 2000) 233 F3d 456, 466. To evaluate the likelihood of confusion in cases involving fanciful marks, courts typically consider the following factors (233 F3d at 461):

- The mark's inherent distinctiveness;
- The degree to which the goods are similar in use and function;
- Similarity of the marks;
- Evidence of actual confusion;
- Marketing channels used;
- Type of goods and the degree of care likely to be exercised by the purchaser;
- Defendant's intent in selecting the mark; and
- Likelihood of expansion of the product lines.

See also *Playboy Enters. v Netscape Communications Corp.* (9th Cir 2004) 354 F3d 1020, 1026; *AMF Inc. v Sleekcraft Boats* (9th Cir 1979) 599 F2d 341, 348. Relying on just three factors, the Seventh Circuit found that a likelihood of confusion existed when a website marketing herbal drug alternatives called "Herbrozac," "HerbenolPM," "Herbalium," "Herbaspirin," and "Herbadryl," used trademarks of the famous drugs with similar names in its metatags. The court held that the similarity of the marks, the strength of the plaintiff's mark, and the defendant's intent to confuse supported a finding that the defendant violated the Lanham Act. *Eli Lilly & Co*., 233 F3d at 465.

PRACTICE TIP: Beware of fanciful marks—they are considered strong marks. In the *Natural Answers* case, the defendant changed the letters of the fanciful mark significantly, yet it was still found to be infringing.

© The Regents of the University of California

§3.75 E. Misspellings of Trademarks and Direct Competitors

Leading consumers—however briefly—to a website by using even an inadvertently misspelled version of a competitor's trademark as a metatag may constitute a misappropriation of the competitor's good will. *Prometek Indus. Ltd. v Equitrac Corp.* (7th Cir 2002) 300 F3d 808 (defendant's use of "copitrack," an errant spelling of plaintiff competitor's trademark "copitrac," gave defendant benefit of goodwill associated with plaintiff's trademark). The *Prometek* court found that because plaintiff and defendant companies were direct competitors with similar products, the defendant's use of the plaintiff's trademark in a metatag led to initial interest confusion actionable under the Lanham Act. 300 F3d at 812. Evidence of consumer confusion was not necessary to prove a Lanham Act violation. The court noted that "it is not the case that trademarks can *never* appear in metatags, but that they may only do so where a legitimate use of the trademark is being made." 300 F3d at 814 n3.

© The Regents of the University of California

§3.76 F. "English Words"

Use of trademarks in a generic way or use of trademarks that are considered generic English words may negate a finding of a likelihood of confusion. The plaintiff in *Brookfield Communications, Inc. v West Coast Entertainment Corp*. (9th Cir 1999) 174 F3d 1036 developed and marketed under the trademark "MovieBuff" computer software featuring a searchable database of entertainment-industry related information. The defendant, who had previously registered "moviebuff.com" as a domain name, proposed to offer a similar competing database on the Internet. The Ninth Circuit ruled that the defendant could use the words "movie buff" (with a space) in its metatags because they were words commonly used in the English language to describe a movie devotee. The defendant could not, however, use "MovieBuff" (without a space) because it was not an English word.

PRACTICE TIP: Metatags should be limited to words found in the dictionary. Care should be exercised when using dictionary words that are also third party trademarks to minimize the likelihood of a claim. For example, such words should be used in lower case, without a trademark designation such as ® or .

© The Regents of the University of California

IV. TRADE DRESS

§3.77 A. Introduction

Trade dress is the "total image, design and appearance of a product and may include features such as size, shape, color, color combinations, texture and graphics." *Clicks Billiards, Inc. v Sixshooters, Inc.* (9th Cir 2001) 251 F3d 1252, 1257. It is also protected by trademark law. Trade dress is an expansive concept, and may include design of a children's clothing line (*Wal-Mart Stores v Samara Bros., Inc.* (2000) 529 US 205, 146 L Ed 2d 182, 120 S Ct 1339); the décor, menu, and appearance of a restaurant (*Two Pesos, Inc. v Taco Cabana, Inc.* (1992) 505 US 763, 120 L Ed 2d 615, 112 S Ct 2753; *Fuddruckers, Inc. v Doc's B.R. Others, Inc.* (9th Cir 1987) 826 F2d 837); a faucet design (*Kohler Co. v Moen Inc.* (7th Cir 1993) 12 F3d 632); or the color of a product (*In re Owens-Corning Fiberglas Corp*. (Fed Cir 1985) 774 F2d 1116).

Trade dress may be registered with the U.S. Patent and Trademark Office following the same procedures as trademarks. See generally TMEP ¶¶1202.02-1202.02(e). Trademark registration procedures are discussed in §§3.30-3.44. Like a trademark, trade dress must identify the source of the product to be eligible for protection under the Lanham Act. *Fabrication Enters. v Hygenic Corp.* (2d Cir 1995) 64 F3d 53, 58. In general, there are two types of trade dress: product packaging and product design or configuration. *Two Pesos, Inc. v Taco Cabana, Inc.* (1992) 505 US 763, 120 L Ed 2d 615, 112 S Ct 2753; *Wal-Mart Stores v Samara Bros., Inc.* (2000) 529 US 205, 215, 146 L Ed 2d 182, 191, 120 S Ct 1339.

Section 43(a)(3) of the Lanham Act (15 USC §1125(a)(3)) allows suits for infringement of unregistered trade dress if the plaintiff sustains the burden of proof that the matter sought to be protected is not functional. For further discussion of the concept of functionality, see §§3.80-3.83.

© The Regents of the University of California

§3.78 B. Website User Interfaces

Trade dress protection is typically sought by product manufacturers in order to protect the unique packaging or other configuration of their products. The software industry, however, has attempted to avail itself of the benefits of trade dress protection in connection with certain elements of software programs such as user interfaces. The user interface of software programs has been described as "the means by which the software and user interact" and "the sequence of the screens and the choices presented, the layout of the screens, and the method of feedback to the user." See Kellner, *Trade Dress Protection for Computer User Interface "Look and Feel,"* 61 U Chi L Rev 1011, 1012 (Summer 1994) and cases cited therein. The user interface is sometimes referred to as the "look and feel" of the software. See, *e.g.*, *Integral Systems, Inc. v Peoplesoft, Inc*. (ND Cal, July 19, 1991) 1991 US Dist LEXIS 20878**.** To date, there are apparently no reported cases on the applicability of trade dress protection to website user interfaces, although trade dress infringement claims have been made in several actions involving software programs, with uneven results. For example, in *Interactive Network, Inc. v NTN Communications* (ND Cal 1995) 875 F Supp 1398, the court ruled that an interactive video game was not entitled to trade dress protection because the features sought to be protected were functional features. See 15 USC §1125(a)(3) (nonfunctionality requirement for protection of unregistered trade dress).

Copying a user interface may result in a copyright infringement claim and also potentially, a trade dress infringement claim. Trade dress law is evolving, and because copyright cases have limited the scope of protection of website user interfaces (see, *e.g., Lotus Dev. Corp. v Borland Int'l, Inc.* (1st Cir 1995) 49 F3d 807, aff'd by an equally divided court (1996) 516 US 233 (computer software menu command hierarchy is uncopyrightable method of operation, not copyrightable subject matter))*,* trade dress law may be an appropriate avenue to pursue.

PRACTICE TIP: When hiring a website developer, it is a good idea to obtain an indemnification agreement covering not only patent and copyright infringement claims but also claims for infringement of third party intellectual property rights in general, including trade dress.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/3 Domain Names and Trademark Issues/§3.79 C. Trade Dress Infringement

§3.79 C. Trade Dress Infringement

Following are the elements of a claim of trade dress infringement (*Clicks Billiards, Inc. v Sixshooters, Inc.* (9th Cir 2001) 251 F3d 1252, 1258):

- The plaintiff's trade dress is not functional;
- The plaintiff's trade dress operates to identify its source because it is inherently distinctive or has acquired a secondary meaning; and
- The defendant's product or service creates a likelihood of confusion.

See also *Two Pesos, Inc. v Taco Cabana, Inc.* (1992) 505 US 763, 769, 120 L Ed 2d 615, 624, 112 S Ct 2753. These elements are discussed further in §§3.80-3.87.

© The Regents of the University of California

1. Nonfunctionality

§3.80 a. Overview

Trade dress is not protected if a product's design, packaging, color, or other visual characteristics are merely functional. A product's design or appearance is functional if it is "essential to the use or purpose of the product or if it affects the cost or quality of the product." *TrafFix Devices, Inc. v Marketing Displays, Inc.* (2001) 532 US 23, 28, 149 L Ed 2d 164, 177, 121 S Ct 1255. A product's functional aspects are protected by patent law, not trade dress law, because "the functionality doctrine prevents trademark law, which seeks to promote competition by protecting a firm's reputation, from instead inhibiting legitimate competition by allowing a producer to control a useful product feature." *Qualitex Co. v Jacobson Prods. Co.* (1995) 514 US 159, 164, 131 L Ed 2d 248, 254, 115 S Ct 1300.

Courts have struggled in analyzing whether a product feature is purely functional or whether it serves to identify the source of the product. As the Ninth Circuit explained in *Fuddruckers, Inc. v Doc's B.R. Others, Inc.* (9th Cir 1987) 826 F2d 837, 842, the inquiry into functionality is addressed not to "whether the individual elements of the trade dress fall within the definition of functional, but to whether the whole collection of elements taken together are functional." 826 F2d at 842.

© The Regents of the University of California

§3.81 b. Four-Factor Test for Functionality

The Ninth Circuit uses a four-factor test to determine whether trade dress design is functional (*Disc Golf Ass'n Inc. v Champion Disc, Inc.* (9th Cir 1998) 158 F3d 1002, 1006):

- Whether the design yields a utilitarian advantage;
- Whether alternative designs are available;
- Whether advertising touts the utilitarian advantages of the design; and
- Whether the particular design results from a comparatively simple or inexpensive. method of manufacture.

No single factor is dispositive; all must be considered together. 158 F3d at 1006. In *Disc Golf Ass'n,* the court found that the plaintiff failed to overcome the "weighty evidence" of functionality inherent in an expired utility patent. 158 F3d at 1006. Commenting on the interplay between utility patents and trademark protection, the court quoted McCarthy, McCarthy on Trademarks and Unfair Competition §7:89 at 7-208 (4th ed 1996) (158 F3d at 1008):

> A kind of estoppel arises. That is, one cannot argue that a shape is functionally advantageous in order to obtain a utility patent and later assert that the same shape is non-functional in order to obtain trademark protection.

© The Regents of the University of California

§3.82 c. Doctrine of Aesthetic Functionality

One aspect of the functionality doctrine is "aesthetic functionality." In general, the functionality doctrine applies to utilitarian features. According to some courts, however, the doctrine of functionality "has not been limited to those features that are strictly utilitarian." *Keene Corp. v Paraflex Indus., Inc.* (3d Cir 1981) 653 F2d 822, 824. The Restatement (Third) of Unfair Competition explains that "when aesthetic considerations play an important role in the purchasing decisions of prospective consumers, a design feature that substantially contributes to the aesthetic appeal of a product may qualify as 'functional.'" Restatement (Third) of Unfair Competition, §17, Comment b, Illustration c (1995). The doctrine of aesthetic functionality denies trademark protection for designs such as a candy box in the shape of a heart or a "distinctive printing type face." McCarthy, McCarthy on Trademarks and Unfair Competition §7:79 (4th ed 1996). A design may deemed functional if it satisfies the purchaser's "demand for the aesthetic as well as for the utilitarian." *Pagliero v Wallace China Co*. (9th Cir 1952) 198 F2d 339, 344. Most courts have rejected the "aesthetic functionality" doctrine, and it is not clear whether courts in California will continue to apply it. Courts that have rejected or limited the use of this doctrine include *Keene Corp. v Paraflex Indus., Inc., supra,* and *Sicilia Di R. Biebow & Co. v Cox* (5th Cir 1984) 732 F2d 417. See also *Big Island Candies, Inc. v Cookie Corner* (D Haw 2003) 244 F Supp 2d 1086.

© The Regents of the University of California

§3.83 d. Functionality and Website User Interfaces

Courts have not addressed the functionality of trade dress in the context of website user interfaces, although the concept has been applied to computer software. See, *e.g., Interactive Network, Inc. v NTN Communications* (ND Cal 1995) 875 F Supp 1398 (interactive video game). In that case, the court remarked that even though individual features of a product may be functional when considered separately, as a whole they may be nonfunctional if they "serve to distinguish the product from rival products rather than being necessary to the product's use." 875 F Supp at 1406. The extent to which a website user interface might be considered functional and therefore not protectable as trade dress is unclear. Purely functional elements such as navigation bars and shopping carts, may not be protectable as trade dress, although the same elements might qualify for a business method patent. See, *e.g., Amazon.com, Inc. v Barnes & Noble.com, Inc.* (Fed Cir 2001) 239 F3d 1343 ("one-click" purchasing feature). For a discussion of business method patents, see §2.18. Some user interfaces contain more functional features than others. It is likely that the more interactive a feature is, the more likely it would be considered functional. Static graphic designs are more likely to be viewed as nonfunctional.

© The Regents of the University of California

2. Inherent Distinctiveness or Secondary Meaning

§3.84 a. Inherent Distinctiveness Test

To obtain protection under the Lanham Act, trade dress, like a trademark, must either be inherently distinctive or else have acquired a secondary meaning that distinguishes the claimant's goods in commerce. See generally *Two Pesos, Inc. v Taco Cabana, Inc.* (1992) 505 US 763, 769, 120 L Ed 2d 615, 623, 112 S Ct 2753.

Section 43(a) of the Lanham Act (15 USC §1125(a)) protects trade dress that is inherently distinctive, even if it has not acquired a secondary meaning. 505 US at 772, 120 L Ed 2d at 626 (restaurant motif, including "festive eating atmosphere, artifacts, bright colors, paintings, murals," exterior, and server uniforms constituted protectable trade dress). In *Two Pesos,* the Court explained that if trade dress is "capable of identifying products or services as coming from a specific source," it is inherently distinctive, and proof of secondary meaning is not required. There is no reason to treat trade dress differently from other indicators of source or origin. 505 US at 773, 120 L Ed 2d at 627.

© The Regents of the University of California

§3.85 b. Product Designs and Product Packaging

Any mark that consists of a product design is not registrable on the principal register unless it is established that the mark has acquired distinctiveness. *Wal-Mart Stores v Samara Bros., Inc.* (2000) 529 US 205, 210, 146 L Ed 2d 182, 188, 120 S Ct 1339. Wal-Mart sold garments with a design similar to those sold in Samara Brothers' stores; Samara Brothers did not register a product design trade dress. The court held that product designs are never inherently distinctive because they are generally not a source identifier and that the owner of an unregistered product design trade dress under the Lanham Act must prove that the design has acquired a secondary meaning. 529 US at 216, 146 L Ed 2d at 192. The court made it clear, however, that product packaging case law would still apply, and that product packaging can be inherently distinctive. Although the trade dress at issue was unregistered, some commentators have suggested the *Samara Brothers* holding should apply in Trademark Trial and Appeal Board decisions. McCarthy, McCarthy on Trademarks and Unfair Competition §8:12.1 (4th ed 1996).

Other courts have also indicated that it may be less difficult to prove distinctiveness for product packaging than for product design. *Landscape Forms, Inc. v Columbia Cascade Co.* (2d Cir 1997) 113 F3d 373, 379 ("*[t]*his circuit appears to be moving toward a rule that packaging is usually indicative of a product's source, while the design or configuration of the product is usually not so"); *Big Island Candies, Inc. v Cookie Corner* (D Haw 2003) 269 F Supp 2d 1236. Because of the difficulty of proving a secondary meaning, counsel should try to characterize the trade dress as product packaging. Not all trade dress can be neatly characterized as either product design or product packaging, however. In cases where it is not clear what type of trade dress is involved, courts will most likely classify the trade dress as product design. As one court explained, in close cases "courts should err on the side of caution and classify ambiguous trade dress as product design, thereby requiring secondary meaning." *Wal-Mart Stores v Samara Bros., Inc.* (2000) 529 US 205, 215, 146 L Ed 2d 182, 192, 120 S Ct 1339.

© The Regents of the University of California

§3.86 c. Website User Interfaces: Product Design or Product Packaging?

It is not yet clear whether website user interfaces constitute product packaging trade dress or product design trade dress. A website user interface for a retail distributor with no physical presence may be the only "storefront" for the business. Website user interfaces display unique graphical designs, colors, and even sounds that may constitute a "motif" analogous to the trade dress at issue in *Two Pesos, Inc. v Taco Cabana, Inc.* (1992) 505 US 763, 772, 120 L Ed 2d 615, 626, 112 S Ct 2753. In *Two Pesos,* the trade dress included the restaurant's color scheme, artifacts, festive atmosphere, umbrellas, and murals. Using the same reasoning, a court might find that a website user interface is product packaging trade dress and inherently distinctive. As the Internet continues to develop as a venue for mainstream commercial activity and consumer branding, trade dress protection for websites is likely to become more important—and therefore a basis for potential infringement claims between competitors.

© The Regents of the University of California

§3.87 3. Likelihood of Confusion in Trade Dress

In *Clicks Billiards, Inc. v Sixshooters, Inc.* (9th Cir 2001) 251 F3d 1252, 1264, the Ninth Circuit held that likelihood of confusion is the most important element of proof in a trademark infringement action. A likelihood of confusion exists when "customers viewing the mark would probably assume that the product or service it represents is associated with the source of a different product or service identified by a similar mark." 251 F3d at 1265.

The factors to consider in determining whether a likelihood of confusion exists are as follows (*Clicks Billiards, Inc. v Sixshooters, Inc.* (9th Cir 2001) 251 F3d 1252, 1265; *Fuddruckers, Inc. v Doc's B.R. Others, Inc.* (9th Cir 1987) 826 F2d 837, 845):

- Evidence of actual confusion;
- Defendant's intent in using the mark;
- Similarity of marks;
- Similarity of goods;
- Similarity of marketing channels; and
- Strength of the mark.

For evidence of actual confusion, a consumer survey may be sufficient. In *Clicks Billiards,* the plaintiff asserted that the defendant infringed its trade dress with respect to the motif of its billiard halls. The plaintiff was able to show actual proof of a likelihood of confusion through a survey that asked customers if they thought the defendant's and plaintiff's billiard halls were owned by the same company. 251 F3d at 1262. See also *Libman Co. v Vining Indus.* (7th Cir 1995) 69 F3d 1360, 1364, cert denied (1996) 517 US 1234 (plaintiff's claim of consumer confusion, absent survey, could not "be regarded as better than a hypothesis, and a hypothesis that has not been tested").

In trade dress cases, all elements of the product design or product package may be considered features that identify the product. In *Clicks Billiards,* the defendant asserted trade dress rights in numerous elements of the interior design of its billiard hall, including the large floral print carpet pattern and style, the dark mahogany wood finish, ceiling and wall coverings, the design of custom lighting fixtures, layout of pool tables, cue racks, and the wood trim on top of the dark green acoustical wall. 251 F3d at 1256. In preparing a trade dress infringement case, listing all of the elements that comprise the trade dress should help demonstrate to the court that the trade dress is unique and identifiable and that, if copied, confusion may result.

© The Regents of the University of California

4

Human Resources

I. EMPLOYEES AND EMPLOYMENT ISSUES
- A. Introduction §4.1
- B. Ethical Considerations §4.2
- C. "At Will" Employment §4.3
- D. Offer Letter to Prospective Employee
  - 1. Introduction §4.4
  - 2. Form: Offer Letter to Prospective Employee §4.5
- E. Confidentiality and Invention Assignment Agreements
  - 1. Employee Confidentiality Agreements §4.6
  - 2. Employee Inventions §4.7
    - a. Federal "Work for Hire" Doctrine §4.8
    - b. Employer Ownership of Employee Inventions Under State Law §4.9
  - 3. Invention Assignment Agreements §4.10
  - 4. Form: Confidentiality and Invention Assignment Agreement §4.11
- F. Employee Overtime—Special Rules for Computer Programmers §4.12

II. INDEPENDENT CONTRACTORS
- A. Introduction §4.13
- B. Classification of Independent Contractors §4.14
  - 1. Behavioral Control §4.15
  - 2. Financial Control §4.16
  - 3. Type of Relationship §4.17
- C. Intellectual Property Issues in Independent Contractor Relationships §4.18
- D. Form: Independent Contractor Consulting Agreement §4.19
- E. Independent Contractor Nondisclosure Agreement
  - 1. Introduction §4.20
  - 2. Form: Nondisclosure Agreement §4.21

III. ADVISORY BOARDS
- A. Introduction §4.22
- B. Form: Advisory Board Letter Agreement §4.23

© The Regents of the University of California

I. EMPLOYEES AND EMPLOYMENT ISSUES

§4.1 A. Introduction

Sections 4.2-4.12 focus on basic employment issues for companies developing and operating Internet websites. Clear and thorough employment documentation is necessary to avoid confusion and potential disputes regarding terms of employment and intellectual property allocation and ownership issues. Because employees are the primary source of the creation of new value for a company (by developing client relationships, creating intellectual property, and keeping historical knowledge about the company and its operations), proper documentation will aid in securing for the company's benefit the value that the employees create during the course of their employment.

There are generally two models for contracting for an employment relationship. For certain types of employees, such as those with more common skill-sets, a company may decide not to enter into any formal employment agreement, preferring not to be bound to specific terms or to undergo the expense of drafting and negotiating a full agreement for each employee. For these types of employees, companies may choose to use an "at will" offer letter containing flexible employment terms established in the employer's discretion. See §4.5.

For more senior staff or employees with scarce skill-sets, a company may prefer to use a longer form of employment agreement for a term of years with more specific terms and conditions. Senior executives, who are often company founders, may have skills and expertise that make them key to the company's continued research and development activities, growth, or market success. The company may want some assurance of access to the individual's services for a period of time, and the individual, in turn, may desire assurance of certain minimum levels of compensation and benefits to be willing to forgo other offers of employment. For more complete discussion and analysis of longer forms of employment agreements, see Advising California Employers and Employees (Cal CEB 2005).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/4 Human Resources/§4.2 B. Ethical Considerations

§4.2 B. Ethical Considerations

Attorneys often work closely with company founders and executives as the primary representatives of their client organizations. When dealing with matters related to the employment of a founder or executive, however, the employee becomes an adverse party. This shift in the attorney/client relationship brings with it the potential for miscommunication and ethical concerns, such as conflicts of interest. Furthermore, if the client's employee is not represented by separate counsel, the employee may misunderstand the role of company counsel and believe mistakenly that company counsel is looking out for the employee's best interests.

California Rules of Professional Conduct 3-310 addresses the representation of conflicting interests, stating that:

> A member shall not accept or continue representation of a client without providing written disclosure to the client where: (1) The member has a legal, business, financial, professional, or personal relationship with a party or witness in the same matter.

Company counsel should take care in discussions or negotiations with employees not to give the impression that counsel is providing legal advice to them. The attorney should remain aware of the potential for misunderstanding on the part of an employee and rectify any misunderstanding that occurs. ABA Model Rule 4.3 states:

> In dealing on behalf of a client with a person who is not represented by counsel, a lawyer shall not state or imply that the lawyer is disinterested. When the lawyer knows or reasonably should know that the unrepresented person misunderstands the lawyer's role in the matter, the lawyer shall make reasonable efforts to correct the misunderstanding.

Company counsel should also consider whether to encourage the employee to seek separate counsel. The employer-client may be reluctant to do so, perhaps due to a concern that the employer may have to absorb the cost of separate counsel or a fear that delays will result from the involvement of separate counsel. The attorney should educate the employer-client that having separate representation for the employee should aid in the ultimate enforceability of the agreement. Civil Code §1654 provides that "the language of a contract should be interpreted most strongly against the party who caused the uncertainty to exist." In many cases, the employer's counsel drafts the agreement without input from opposing counsel and may be deemed to have "caused" any uncertainties.

© The Regents of the University of California

§4.3 C. "At Will" Employment

Labor Code §2922 provides that an employment having no specified term "may be terminated at the will of either party on notice to the other." If there is no agreement to the contrary, Lab C §2922 creates a presumption of at-will employment. The presumption of at-will employment may be overcome by evidence that the employer's right to terminate the employment at will has been limited in some way. *Foley v Interactive Data Corp.* (1988) 47 C3d 654, 677, 254 CR 211; *Nelson v United Technols.* (1999) 74 CA4th 597, 615, 88 CR2d 239. Evidence that a court might consider to rebut the presumption of an at-will relationship includes (see *Foley,* 47 C3d at 677):

- The contents of personnel policies;
- Past practice by the employer;
- The length of the employee's service;
- Industry practice; and
- Acts or communications by the employer assuring continued employment.

Thus, it is important for employers to construct agreements with their employees carefully and to maintain and circulate policy statements to reduce the risk of possible claims by employees that continued employment is assured or that the at-will nature of the relationship has been changed.

© The Regents of the University of California

D. Offer Letter to Prospective Employee

§4.4 1. Introduction

In §4.5 is a sample letter to be used for potential employees to establish the at-will nature of employment with the company and other basic terms of employment. This form is typically prepared on company letterhead addressed to the employee, to be countersigned and returned by the employee to indicate acceptance of the offer.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/4 Human Resources/§4.5 2. Form: Offer Letter to Prospective Employee

§4.5 2. Form: Offer Letter to Prospective Employee

▶ To download **Word** version, right click and choose *Save Target As*

▶ To download **WordPerfect** version, right click and choose *Save Target As*

[*Company letterhead*]

_ _[*Date*]_ _

_ _[*Employee's name and address*]_ _

Re: Terms of employment

Dear _ _[*name of employee*]_ _:

This letter is intended to set forth in writing the terms of our offer for you to join _ _[*name of company*]_ _ (the "Company") as an employee. This letter sets forth the terms of the offer, which, if you accept by signing below and returning the signed original to me by 5:00 pm on _ _[*date*]_ _, will govern your employment with the Company.

1. POSITION AND DUTIES. Your initial position will be _ _[*position*]_ _ reporting to the _ _[*title of manager for this position*]_ _ of the Company. Your specific duties and responsibilities will be determined by the Company's management from time to time.

Comment: If the company has specific initial goals or objectives for the employee, they should be clearly detailed in this section. Note that in this sample clause, the description of title and duties is not fixed and management has flexibility to determine the employee's specific job duties over time. This approach mitigates against the possibility that a change in duties or title may give rise to a claim for constructive termination. *Turner v Anheuser-Busch* (1994) 7 C4th 1238, 32 CR2d 223; *Addy v Bliss & Glennon* (1996) 44 CA4th 205, 218, 51 CR2d 642.

2. START DATE. Your start date with the Company will be _ _[*date*]_ _.

3. COMPENSATION. Your initial annual salary will be _ _[*dollar amount*]_ _, payable in accordance with the Company's payroll policies. You will be considered for promotions and compensation adjustments in accordance with the Company's policies in effect from time to time.

4. BONUS PROGRAM. You will be eligible for an annual, performance-based bonus, which will be tied to an annual performance review on your anniversary date. This bonus will be payable at such times as determined by the board of directors of the Company. The bonus amounts will be determined at the Company's discretion.

5. BENEFITS. You will be entitled to participate in the health and other benefit plans of the Company pursuant to their terms, as they may be amended from time to time by the Company, and made available to similarly situated employees.

6. VACATION. You will receive _ _[*number of days*]_ _ days paid vacation per year in accordance with the Company's vacation policy (to be scheduled and approved in advance).

7. STOCK OPTIONS. You will be granted options to acquire _ _[*number*]_ _ shares of the Company's common stock pursuant to the Company's Equity Incentive Plan dated _ _[*date*]_ _ subject to your execution of a stock option agreement to be provided to you by the Company, along with a copy of the plan, within _ _[*number*]_ _ days after your delivery of this letter, countersigned by you, back to the Company. The exercise price of your options will be _ _[*dollar amount*]_ _ per share and the options will vest in equal installments over _ _[*number*]_ _ years. The stock option agreement will contain the Company's standard stock restriction provisions. To be effective, the stock option agreement must be executed and returned by you within _ _[*number*]_ _ days after your receipt of the agreement.

8. POLICIES. You agree to abide by and comply with the policies of the Company that are in force from time to time.

9. AT-WILL EMPLOYMENT. Your employment with the Company will be at will, and therefore may be terminated by you or the Company at any time, with or without cause and with or without notice. You understand that the at-will employment relationship will remain in effect throughout your employment with the Company, unless modified by an express written contract for a specified term signed by an authorized representative of the Company and you. You further understand that the at-will employment relationship may not be modified by any oral or implied agreement.

Please initial to indicate that you have read and understand this paragraph: _____

Comment: This language confirms the employee's understanding of the at-will nature of the relationship. Having the employee separately initial this section serves to draw the employee's attention to the clause, gives the employee a chance to raise any questions that he or she may have, and serves as evidence that the parties knowingly agreed to at-will employment, in the event of a future dispute.

10. FULL-TIME EMPLOYMENT. You will devote your full professional time and attention to the performance of your duties for the Company. We ask that you devote your best efforts to the interests of the Company and that you not, without the prior written consent of an authorized representative of the Company, engage (a) in any other employment or services for a third party, or (b) in any activities detrimental to the best interests of the Company.

Comment: Consider whether any further limitations (such as restricting ownership of stock of competing nonpublic companies, or serving on boards of directors or advisory boards of other companies without the employer's consent) are in order. Employees with unique or recognized technical expertise may wish to serve on boards of trade associations or teach courses at academic institutions. This section may include pre-approval of specific activities to the extent that the employee is engaging in them at the time the agreement is entered into. Future outside activities that could detract from the employee's ability to perform on a full-time basis should be reviewed on a case-by-case basis.

11. OTHER AGREEMENTS. As a condition to your employment, you will be required to sign the Company's Employee Confidentiality and Assignment of Inventions Agreement. A copy of this document is included with this letter for you to sign and return in order for your employment relationship with the Company to be effective.

Comment: If there are other documents or agreements to be signed by the employee in connection with the commencement of employment (such as a confirmation of receipt of an employee manual), they should be listed in this section.

12. RELIANCE. In making this offer, we are relying on the information you have provided to us about your background and experience, including any information provided to us in any employment application you may have submitted to us. You confirm, by executing this letter, the truth and accuracy of all statements you have made to the Company.

13. COMPLETE AGREEMENT. On your acceptance of this letter, it will contain the entire agreement and understanding between you and the Company (along with the Stock Option Plan, Stock Option Agreement, Confidentiality Agreement, and other policies established from time to time by the Company). This letter supersedes any prior or contemporaneous agreements or understandings by or on behalf of the Company, whether oral or in writing.

Comment: If any additional documents are added to Paragraph 11 above, they should also be added here.

If the above terms and conditions are acceptable to you, please countersign this letter where indicated below and return it to us. We are very much looking forward to having you as part of _ _[*name of company*]_ _.

Very truly yours,

Date: _ _ _ _ _ _ _ _[*NAME OF COMPANY*]_ _**,**

a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

AGREED AND ACCEPTED:

Date: _ _ _ _ _ _ __[*Signature*]__
_ _[*Typed name of employee*]_ _

© The Regents of the University of California

E. Confidentiality and Invention Assignment Agreements

§4.6 1. Employee Confidentiality Agreements

An employee confidentiality agreement serves several purposes. First, the existence of such agreements serves to support the trade secret status of the company's confidential business information. The Uniform Trade Secrets Act (UTSA) (CC §§3426-3426.11) governs claims of trade secret misappropriation. A trade secret is defined as (CC §3426.1(d)):

> information, including a formula, pattern, compilation, program, device, method, technique, or process that: (1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

The execution of an employee confidentiality agreement is evidence that the company is taking reasonable measures to ensure the confidentiality of its trade secret information. Further, the execution of a confidentiality agreement reminds employees of their obligations of confidentiality and puts them on notice of their duties to their employer. In addition, outside investors typically require such agreements to protect their interests, and having them in place from the company's beginning in a consistent manner supports the value of the company's intellectual property. See generally Trade Secrets Practice in California (2d ed Cal CEB 1996); Financing and Protecting California Businesses (Cal CEB 2006).

Although it is possible to insert the terms of a confidentiality and invention assignment agreement into the text of an offer letter, employment agreement, or policy handbook, these terms should be viewed as ancillary and should be the subject of a separate agreement. A separately signed agreement can more easily be subject to due diligence review without disclosing the confidential elements of an employment agreement and will more clearly evidence that the employee has read and understood its specific terms.

© The Regents of the University of California

§4.7 2. Employee Inventions

As a general rule, an inventor owns the product of his or her invention. Civil Code §980 provides:

> The author of any original work of authorship that is not fixed in any tangible medium of expression has an exclusive ownership in the representation or expression thereof as against all persons except one who originally and independently creates the same or similar work.

At common law, any inventions made on the job by an employee belonged to the employee *unless* the employee was hired or assigned to invent. See *U.S. v Dubilier Condenser Corp*. (1933) 289 US 178, 77 L Ed 1114, 53 S Ct 554; *Lion Mfg. Corp. v Chicago Flexible Shaft Co*. (9th Cir 1939) 106 F2d 930. The employer, however, is deemed to have an implied nonexclusive and nontransferable license (or "shop right") to use any such employee invention developed outside the scope of the employee's job duties, if employer resources also contributed to the invention. *U.S. v Dubilier Condenser Corp., supra*. See Trade Secrets Practice in California §§2.6-2.9 (2d ed Cal CEB 1996).

Several statutes and cases, however, make clear that the employer owns outright any inventions or work product of an employee made within the scope of the employee's employment. See §§4.8-4.9.

© The Regents of the University of California

§4.8 a. Federal "Work for Hire" Doctrine

Under federal copyright law, a "work made for hire" is a work prepared by an employee within the scope of his or her employment. 17 USC §101. The employer for whom the work was prepared is considered the author of the copyrighted work, and, unless the parties have expressly agreed otherwise in a written instrument signed by them, the employer owns all of the rights included in the copyright. 17 USC §201(b). For further discussion of the "work for hire" doctrine, see §1.5.

© The Regents of the University of California

§4.9 b. Employer Ownership of Employee Inventions Under State Law

Labor Code §2860 provides that:

> Everything which an employee acquires by virtue of his employment, except the compensation which is due to him from this employer, belongs to the employer, whether acquired lawfully or unlawfully, or during or after the expiration of employment.

Section 2870(a) also supports employer ownership of employee inventions. This statute provides for employer ownership of inventions that either:

> (1) Relate at the time of conception or reduction to practice of the invention to the employer's business, or actual or demonstrably anticipated research or development of the employer; or (2) Result from any work performed by the employee for the employer.

It is therefore clear under California statutes that any inventions developed by an employee in the course of or in connection with his or her employment are the property of the employer.

California case law is consistent. In *Treu v Garrett Corp.* (1968) 264 CA2d 432, 70 CR 284, defendant Garrett Corporation received an assignment of the exclusive rights to a patent from its holder. Later, the former patent holder was hired by Garrett for the express purpose of developing improvements to the original patent. The former holder did so, but a dispute arose concerning ownership of the improvements. The court held that Garrett owned the improvements because they were developed by the original holder while he was employed at Garrett. The improvements were the very thing for which the original holder was hired and paid. In *Daniel Orifice Fitting Co. v Whalen* (1962) 198 CA2d 791, 18 CR 659, the defendant had been hired to develop improvements to the plaintiff's manufactured products. The defendant developed certain improvements but did not disclose them to his employer because he intended to use them later, in competition with his employer. The court found that the improvements belonged to the employer because their development was within the scope of the employee's employment (198 CA2d at 797):

> Where a person is employed to design improvements to the product of his employer, or to design new products for his employer, and he does so, he may not use the results of such work for his own use and benefit, and particularly not to the detriment of his employer.

© The Regents of the University of California

§4.10 3. Invention Assignment Agreements

The issue of ownership of inventions and improvements to company technology is vitally important to technology and Internet businesses that rely on intellectual property as the foundation of their intrinsic corporate value as well as the value of their products sold in the marketplace. Accordingly, technology and Internet companies commonly require their employees to execute invention assignment agreements as a condition of their employment. In *Iconix, Inc. v Tokuda* (ND Cal 2006) 457 F Supp 2d 969, the court enforced an invention assignment agreement and enjoined the defendants from operating a commercial website that they conceived, constructed, and launched on their former employer's time using their former employer's copyrighted software.

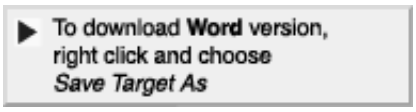
Invention assignment agreements have certain statutory limitations in California. Labor Code §2870(a) precludes employers from requiring employees to assign inventions that are unrelated to the employee's employment, *i.e.,* developed on the employee's own time and without using the employer's equipment, supplies, facilities, or trade secrets. Employment agreement provisions purporting to require an employee to assign an invention that is excluded by Lab C §2870(a) are unenforceable. Lab C §2870(b).

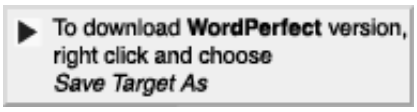
A form of employee confidentiality and invention assignment agreement is in §4.11.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/4 Human Resources/§4.11 4. Form: Confidentiality and Invention Assignment Agreement

§4.11 4. Form: Confidentiality and Invention Assignment Agreement





EMPLOYEE NONDISCLOSURE AND INTELLECTUAL PROPERTY ASSIGNMENT AGREEMENT

This Nondisclosure and Intellectual Property Assignment Agreement (this "Agreement") is entered into and made effective as of _ _[*date*]_ _ (the "Effective Date), between _ _[*company name*]_ _, a California corporation ("Company"), and _ _[*employee name*]_ _ ("Employee") with respect to the following:

Comment: This agreement should be entered into as of the employment start date, and no later, to avoid any gaps in the time period of its coverage.

A. Company possesses considerable know-how and proprietary intellectual property rights relating to, without limitation, _ _[*describe subject area of company business*]_ _ and related technology.

B. Company and Employee have entered into this Agreement to assure the confidentiality of information provided by Company to Employee, generated by Employee, or of which Employee otherwise becomes aware.

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. DEFINITION OF CONFIDENTIAL INFORMATION. The term "Confidential Information" as used in this Agreement means all information disclosed by Company to Employee, as well as any information to which Employee has access or that is learned, generated, or created by Employee, whether alone or jointly with others. Confidential Information includes, but is not limited to, source code and programming information, and all marketing, operational, technical, economic, or financial knowledge, information, or data of any nature whatsoever relating to the business of Company, which has been or may hereafter be learned, generated, created, or otherwise obtained by Employee, alone or jointly with others, whether in written, electronic, oral, or any other form. Confidential Information shall also include any information that is provided to Company by third parties and is subject to obligations of confidentiality.

Comment: Counsel should consider tailoring the definition of confidential information more specifically to the types of intellectual property that may be generated by the company's business. Because employees may gain access to confidential information of third parties such as customers and vendors, it is important to clarify that third party information must be kept confidential also.

2. EXCEPTIONS TO DEFINITION OF CONFIDENTIAL INFORMATION. Confidential Information shall not include the following:

(a) Information that is publicly available at the time of disclosure, or information that later becomes publicly available through no act or omission of Employee;

(b) Information that Employee can demonstrate was in Employee's possession before the date of commencement of Employee's employment with Company; or

(c) Information disclosed to Employee by a third party not in violation of any obligation of confidentiality to Company.

3. DISCLOSURE AND USE OF CONFIDENTIAL INFORMATION. Employee shall use the Confidential Information only for the purpose of performing Employee's duties to Company within the course and scope of Employee's employment, and shall make no use or disclosure of the Confidential Information, in whole or in part, for any other purpose. Employee agrees to keep confidential all Confidential Information and to preserve

the confidential and proprietary nature of the Confidential Information at all times. Further, Employee acknowledges that from time to time Company is entrusted with confidential information of third parties and agrees to abide by the terms of any nondisclosure agreements entered into between the Company and such third parties.

Comment: A well written confidentiality agreement restricts both use and disclosure of confidential information. Many agreements cover only disclosure, making them incomplete. Note also the reference to third party confidential information and the need to comply with nondisclosure agreements entered into by the company with third parties.

4. NO OWNERSHIP OR OTHER RIGHTS GRANTED. All right, title, and interest in and to Confidential Information shall remain the property of Company. Nothing in this Agreement shall be construed to grant Employee any rights to or license under the Confidential Information or under any related patent, patent application, trademark, copyright, know-how, or other intellectual property of Company.

5. REQUIRED DISCLOSURE. In the event that Employee is requested or required by subpoena or other court order to disclose any Confidential Information received pursuant to this Agreement, it is agreed that Employee shall provide immediate notice of such request(s) to Company and shall use reasonable efforts to resist disclosure, until an appropriate protective order may be sought, or a waiver of compliance with the provisions of this Agreement granted. If, in the absence of a protective order or the receipt of a waiver hereunder, Employee is nonetheless, in the written opinion of its counsel, legally required to disclose Confidential Information received pursuant to this Agreement, then in such event Employee may disclose such information without liability hereunder, provided that Company has been given a reasonable opportunity to review the text of such disclosure before it is made and that disclosure is limited to only the Confidential Information specifically required to be disclosed.

6. RETURN OF INFORMATION. Employee agrees to return all Confidential Information in Employee's possession on termination of Employee's employment with the Company for any reason, or upon any earlier written request from Company, including all originals, copies, translations, notes, or any other form of said material, without retaining any copy or duplicates thereof, and promptly to delete or destroy any and all written, printed, electronic, or other material or information derived from the Confidential Information.

7. NATURE OF INFORMATION. Employee acknowledges and agrees that the Confidential Information protected by this Agreement is of a special, unique, unusual, extraordinary, and intellectual character; that money damages would not be sufficient to avoid or compensate for the unauthorized use or disclosure of the Confidential Information; and that specific performance, injunctive relief, and other equitable relief would be appropriate to prevent any actual or threatened use or disclosure of the Confidential Information. Employee also acknowledges that the interests of Company in its Confidential Information may be irreparably injured by disclosure of such Confidential Information. The remedies stated above may be pursued in addition to any other remedies available at law or in equity for breach of this Agreement, and Employee agrees to waive any requirement for the securing or posting of any bond in connection with such remedy. Should litigation be instituted to enforce any provision of this Agreement, the prevailing party shall be entitled to recover all costs, including without limitation reasonable legal fees, cost of investigation, and cost of settlement.

8. WORK FOR HIRE. Employee understands and agrees that, to the extent permitted by law, all work, papers, reports, documentation, drawings, images, product ideas, service ideas, photographs, negatives, tapes and masters, computer programs (including their source code and object code), prototypes, and other materials (collectively, "Work Product"), including, without limitation, any and all such Work Product generated and maintained on any form of electronic media, that Employee generates, either alone or jointly with others, during employment with Company shall be considered a "work made for hire," and ownership of any and all copyrights in any and all such Work Product shall belong to Company. In the event that any portion of the Work Product should be deemed not to be a "work made for hire" for any reason, Employee hereby assigns, conveys, transfers, and grants, and agrees to assign, convey, transfer, and grant to Company all of Employee's right, title, and interest in and to the Work Product and any copyright therein, and agrees to cooperate with Company in the execution of appropriate instruments assigning and evidencing such ownership rights under this Agreement. Employee hereby waives any claim or right under the doctrine of "droit moral" (moral right) to object to Company's copyright in or use of the Work Product.

9. INVENTIONS. Employee hereby assigns and agrees to assign to Company all of Employee's right, title, and interest in and to any discoveries, inventions, and improvements (collectively, Inventions), whether patentable or not, that Employee makes, conceives, or suggests, either alone or jointly with others, while

employed by Company. Any Invention that was made, conceived, or suggested by Employee, either solely or jointly with others, within one (1) year following termination of employment with Company and that pertains to any Confidential Information or business activity of Company shall be irrebuttably presumed to have been made, conceived, or suggested in the course of Employee's employment and with the use of the time, materials, or facilities of Company. This Paragraph does not apply to any invention that qualifies under Section 2870 of the California Labor Code, a copy of which is attached hereto as Exhibit A.

Comment: This agreement is structured to create the most protection for the company both by affirming the "work for hire" character of the work performed by the employee and, in case the work-for-hire characterization is not sufficient, by providing for an assignment of all intellectual property created. This double layer of protection is helpful for many reasons. One reason often overlooked is that the copyright law and the work-for-hire doctrine may be difficult for juries to understand, especially if they are dealing with an inventor whose hard work and creativity does not accrue to his personal benefit. Including an assignment clause serves to reinforce the effect of the work-for-hire doctrine.

The one-year "tail" of this agreement (extending its coverage to inventions made or conceived by the employee within one year after employment ends) may be difficult for some employees to accept. This clause has two purposes. First, it recognizes that there is a residual benefit to the employee of the things the employee has learned or done at the company's expense and that creative efforts during the period immediately after separation from the company may have their roots directly in the work that was done for the employer. This clause also serves to address the potential problem of pinpointing with any accuracy exactly when an item of intellectual property was conceived. If an employee knows that he or she will be leaving the company, the employee might argue that key items of intellectual property were conceived a day or two after the effective date of termination. Absent some sort of "tail" period, these issues dilute the effectiveness of the agreement.

The reference to Lab C §2870 in the last sentence of Paragraph 9 is mandatory. Labor Code §2872 provides that:

> If an employment agreement entered into after January 1, 1980, contains a provision requiring the employee to assign or offer to assign any of his or her rights in any invention to his or her employer, the employer must also, at the time the agreement is made, provide a written notification to the employee that the agreement does not apply to an invention which qualifies fully under the provisions of Section 2870.

As a result, every invention assignment agreement entered into with an employee must recite the language of Lab C §2870.

10. ASSISTANCE. Employee shall assist Company and any person designated by it in every proper way and at Company's expense to register, obtain, and enforce Company's rights in Work Product and Inventions. Such assistance shall include, but not be limited to, assistance with and execution of, as applicable, registrations and applications for patent, copyright, or other intellectual property rights in any and all jurisdictions, and execution of further evidence of Employee's assignment of Employee's rights under this Agreement.

[*Add if appropriate*]

11. RETAINED RIGHTS. Exhibit B contains a complete and accurate list of all Inventions related to the subject matter of the Company's business that have been made, conceived, or first reduced to practice by Employee, alone or jointly with others, before the date of commencement of Employee's employment with Company, that are owned by Employee, and that have not been assigned to a prior employer ("Retained Inventions"). Employee does not, by entering into this Agreement, assign to Company any right, title, or interest in the Retained Inventions disclosed on Exhibit B. Employee agrees to obtain Company's written approval before using any Retained Inventions in connection with Employee's work for the Company or incorporating any Retained Inventions into Company work product and, if Employee fails to do so, Employee grants and agrees to grant to Company a fully paid, worldwide, irrevocable, assignable, sublicensable, nonexclusive license to such Retained Invention upon its use or incorporation.

Comment: This provision is optional. Highly skilled employees who are experts in their field may have preexisting inventions that they do not want to transfer to a new employer. It is important, however, for the company to understand in advance what intellectual property the employee claims that he or she owns. Incorporating employee-owned inventions into Company work product may result in a jointly owned work and may give rise to an obligation to share revenues with the employee.

If the company is not able to obtain assurance from the employee that the list in Exhibit B is the entire list of

intellectual property that the employee believes he or she owns, the company might find comfort in relying on the language that requires disclosure and prior approval before use of any such materials on the company's behalf, and the requirement of providing a royalty-free license.

[*Continue*]

[12.] DISCLOSURE OF INVENTIONS. Employee hereby agrees to disclose promptly all Inventions to Company and to perform, during and after Employee's employment, all acts deemed necessary or desirable by Company to permit and assist Company, at its expense, in obtaining and enforcing the full benefits, enjoyment, rights, and title of and to the Inventions throughout the world. Such acts may include, without limitation, the execution and delivery of documents and the provision of assistance or cooperation in legal proceedings. In addition, Employee hereby irrevocably designates and appoints Company and its duly authorized officers and agents as Employee's agent and attorney-in-fact, to act for and in Employee's behalf and stead to execute and file any such applications and to perform all other lawfully permitted acts to further the securing of Company's rights in and to the Inventions.

[13.] NO SOLICITATION. For a period of _ _[*number of years*]_ _ years from the Effective Date, Employee shall not, and shall not assist or encourage others to, directly or indirectly (a) seek to negotiate or influence the terms and conditions of employment of employees of Company or any agreement of collective bargaining with employees of Company; (b) initiate an attempt to employ any person who is an employee of Company; (c) with any person or entity that is a customer of Company, seek to negotiate or influence the terms and conditions of any agreement between such customer and Company; or (d) enter into any discussions, negotiations, arrangements, or understandings with any third party with respect to any of the foregoing.

Comment: A nonsolicitation clause reinforces the employee's duty not to use or disclose the trade secrets of the employer, because customer lists are company trade secrets. This restriction does not, however, mean that the employee is prohibited from working in a similar field or for a competitor after his or her employment with the company ceases. Business and Professions Code §16600 provides: "Except as provided in this chapter, every contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void." Under Bus & P C §16601, covenants not to compete are enforceable to a limited extent in connection with the sale or dissolution of a business, but not in the context of restricting an employee's post-termination activities. See generally Advising California Employers and Employees §§11.51-11.60 (Cal CEB 2005). In this respect, California law differs from the laws of many other jurisdictions. Counsel should take care to inform out-of-state clients of the limitations on their right to restrict the post-termination activities of their California employees.

[14.] AT-WILL EMPLOYMENT. Employee acknowledges and agrees that Employee's employment with Company is at will and, therefore, may be terminated by Employee or by Company at any time, with or without cause and with or without notice. The at-will employment relationship shall remain in effect throughout Employee's employment with Company, unless modified by an express written contract for a specified term signed by Employee and an authorized representative of Company. The at-will employment relationship may not be modified by any oral or implied agreement.

Comment: See the comment in paragraph 9 of the form of Offer Letter to Prospective Employee in §4.5 regarding the advisability of affirming the at-will nature of an employee's employment in any agreement entered into with an at-will employee. If the employee's employment is not at will, this language should be deleted. For general discussion of at-will employment, see §4.3.

[15.] GOVERNING LAW. California law shall govern the interpretation of this Agreement, without reference to rules regarding conflicts of law. Any dispute arising out of this Agreement shall be submitted to a state or federal court sitting in _ _[*specify city and state*]_ _, which shall have the exclusive jurisdiction regarding the dispute and to whose jurisdiction the parties irrevocably submit.

[16.] NO OTHER AGREEMENT. This Agreement, together with its Exhibits, constitutes the parties' entire agreement with respect to the treatment of Confidential Information by Employee and supersedes any and all prior statements or agreements, both written and oral. This Agreement may be amended only by a writing signed by the parties.

[17.] SURVIVAL. This Agreement (a) shall survive Employee's employment with Company, (b) is personal to Employee and may not be assigned by Employee, (c) may be assigned by Company in its sole discretion and

shall inure to the benefit of the successors and assigns of Company, and (d) is binding on Employee's heirs and legal representatives. If Employee's employment with Company is terminated for any reason, Employee consents to the Company's notification of Employee's obligations under this Agreement to any subsequent employer.

[18.] NO WAIVER. No waiver of any term, provision, or condition of this Agreement, whether by conduct or otherwise, in any one or more instances, shall be deemed to be or be construed as a further or continuing waiver of any such term, provision, or condition or as a waiver of any other term, provision, or condition of this Agreement.

[19.] SEVERABILITY. If any court of competent jurisdiction determines any provision of this Agreement to be invalid or unenforceable, such provision shall be interpreted to the maximum extent to which it is valid and enforceable, all as determined by such court in such action, and the remaining provisions of this Agreement shall, nevertheless, continue in full force and effect without being impaired or invalidated in any way.

IN WITNESS WHEREOF, the parties hereto have entered into this Agreement on the day and year first written above.

Date: _ _ _ _ _ _ _ _[*NAME OF COMPANY*]_ _,
a _ _[*state of incorporation*]_ _ **corporation**

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

Date: _ _ _ _ _ _ __[*Signature*]__
_ _[*Typed name of employee*]_ _

EXHIBIT A
California Labor Code §2870

(a) Any provision in an employment agreement which provides that an employee shall assign, or offer to assign, any of his or her rights in an invention to his or her employer shall not apply to an invention that the employee developed entirely on his or her own time without using the employer's equipment, supplies, facilities, or trade secret information except for those inventions that either:

(1) Relate at the time of conception or reduction to practice of the invention to the employer's business, or actual or demonstrably anticipated research or development of the employer; or

(2) Result from any work performed by the employee for the employer.

(b) To the extent a provision in an employment agreement purports to require an employee to assign an invention otherwise excluded from being required to be assigned under subdivision (a), the provision is against the public policy of this state and is unenforceable.

[*Add if optional Paragraph 11 is made part of agreement*]

EXHIBIT B
List of Employee's Retained Inventions

Comment: See paragraph 11 of the Employee Nondisclosure and Intellectual Property Assignment Agreement above for an optional provision regarding the employee's retained rights in inventions made or conceived by the employee before commencement of employment.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/4 Human Resources/§4.12 F. Employee Overtime--Special Rules for Computer Programmers

§4.12 F. Employee Overtime—Special Rules for Computer Programmers

Internet businesses with employees working as software developers must be cognizant of the rules applicable to overtime pay. Under Lab C §510, California employees must receive overtime pay for any work in excess of 8 hours in one day, any work in excess of 40 hours in one week, and for the first 8 hours worked on the seventh day of work in one week. Section 510 does not apply, however, to "exempt employees," which include certain professional, administrative, and executive employees under Lab C §515, and certain surgeons and physicians under Lab C §515.6.

In addition, California has promulgated a special exemption from overtime requirements for employees working in the computer software field under Lab C §515.5. To qualify for the exemption, employers must meet two tests: a "duties" test and a "compensation" test. There are three elements in the "duties" test. The first requires the employee to be "primarily engaged in work that is intellectual or creative and that requires the exercise of discretion and independent judgment." Lab C §515.5(a)(1). The second relates to the specific type of work performed by the employee; he or she must be primarily engaged in one or more of the following (Lab C §515.5(a)(2)):

> (A) The application of systems analysis techniques and procedures, including consulting with users, to determine hardware, software, or system functional specifications.
>
> (B) The design, development, documentation, analysis, creation, testing, or modification of computer systems or programs, including prototypes, based on and related to user or system design specifications.
>
> (C) The documentation, testing, creation, or modification of computer programs related to the design of software or hardware for computer operating systems.

The third element of the "duties" test requires that the employee be highly skilled and proficient in "theoretical and practical application of highly specialized information to computer systems analysis, programming, or software engineering." Lab C §515.5(a)(3).

The "compensation" test requires that the employee be paid not less than a minimum threshold hourly rate, currently set at $36.00 per hour, for every hour worked. The rate for a salaried employee for full-time employment is not less than $75,000, "to be paid at least once a month and in a monthly amount of not less than $6250." Lab C §515.5(a)(4). The threshold amounts for both the hourly wage and the annual salary are adjusted annually. Lab C §515.5(a)(4).

PRACTICE TIP: If an employer intends to avail itself of the exemption under Lab C §515.5, it is important to track employee hours, whether worked at the employer's premises at home, in order to stay in compliance with the "compensation" test. Failure to adhere to the requirements of §515.5 would result in loss of the exemption and resultant liability for additional wages owed under the traditional overtime rules and possible penalties.

The exemption found in §515.5 is not available to employees engaged in the "manufacture, repair or maintenance of computer hardware and related equipment." Lab C §515.5(b)(3). Further, the exemption does not apply to employees who write material such as product descriptions, documentation, promotional material, setup and installation instructions, and similar information for either print or onscreen media, or to employees who prepare content material intended to be read by customers, subscribers, or visitors to computer-related media such as the World Wide Web or CD-ROMs. Lab C §515.5(b)(5). The exemption also does not apply to employees who create imagery for effects used in the motion picture, television, or theatrical industry, regardless of whether computer programming is included in their jobs. Lab C §515.5(b)(6). See generally Advising California Employers and Employees, chap 5 (Cal CEB 2005).

© The Regents of the University of California

II. INDEPENDENT CONTRACTORS

§4.13 A. Introduction

Independent contractors can be an important and valuable tool for companies developing and operating websites. The use of independent contractors can provide companies flexibility and cost effectiveness to meet evolving staffing needs quickly and at lower cost compared with retaining permanent employees. Use of independent contractors also enables companies to take advantage of individuals with specific capabilities for one piece of a large project or an entire short-term project. Moreover, certain individuals in technical fields such as programming may prefer to work independently.

Companies should be aware, however, that the Internal Revenue Service (IRS) and the California Employment Development Department (EDD) are not bound by a company's classification of an individual worker as an independent contractor if the relationship between the company and the individual worker is more analogous to an employer-employee relationship. Misclassification of an employee as an independent contractor can give rise to liability, back taxes, and penalties, as well as an increased risk of being audited by the IRS or EDD. See IRC §3509; IRS Publication 15-A (Employer's Supplemental Tax Guide). See generally Advising California Employers and Employees, chap 3 (Cal CEB 2005).

The factors used by the IRS and EDD to distinguish between independent contractors and employees are discussed in §§4.14-4.17; certain intellectual property issues that arise in connection with the work created by independent contractors are discussed in §4.18. A suggested form for a basic independent contractor consulting agreement is included in §4.19 and a form of nondisclosure agreement for use with independent contractors is included in §4.21.

© The Regents of the University of California

§4.14 B. Classification of Independent Contractors

In *Community for Creative Non-Violence v Reid* (1989) 490 US 730, 751, 104 L Ed 2d 811, 109 S Ct 2166, the Supreme Court held that, in deciding whether a particular worker is an employee or an independent contractor, "we consider the hiring party's right to control the manner and means by which the product is accomplished." Following this rule, both the IRS and the EDD classify workers as independent contractors or employees based on a subjective analysis of who has the right to control the means and methods used to accomplish the subject matter of the work: the worker or the company. See IRS Publication 15-A (Employer's Supplemental Tax Guide) (available at http://www.irs.gov/pub/irs-pdf/p15a.pdf); 22 Cal Code Regs §4304-1. The key distinction is not who *actually* controls (although a company's actual control over a worker is indicative of an employer-employee relationship), but rather which party has the *right* to control, the means and methods of the work. *Smith v Department of Employment* (1976) 62 CA3d 206, 213, 132 CR 874. In general, a worker may properly be classified as an independent contractor if the company has the right to control or direct only the result of the work to be performed and not the means and methods of accomplishing that result. See 22 Cal Code Regs §4304-1. See generally Advising California Employers and Employees, chap 3 (Cal CEB 2005). The IRS examines three general factors (and a number of specific factors within those general areas (see IRS Publication 15-A (Employer's Supplemental Tax Guide))) to decide whether a worker is properly classified as an independent contractor:

- Behavioral control (see §4.15);
- Financial control (see §4.16); and
- The type of relationship (see §4.17).

The EDD, using similar factors as outlined in 22 Cal Code Regs §4304-1, also examines the amount of control a company exercises over its workers to determine whether an independent contractor or employee relationship exists. For both agencies, the three factors listed above are not an exclusive list and no single factor is controlling. See *Tieberg v Unemployment Ins. Appeals Bd.* (1970) 2 C3d 943, 88 CR 175; *California Compensation Ins. Co. v Industrial Acc. Comm'n* (1948) 86 CA2d 861, 195 P2d 880; IRS Publication 15-A (Employer's Supplemental Tax Guide). The IRS and EDD each examine all of the facts and circumstances relevant to the particular worker, the particular company, and the particular industry to properly classify the relationship.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/4 Human Resources/§4.15 1. Behavioral Control

§4.15 1. Behavioral Control

In analyzing whether a company exercises behavioral control over a worker, the IRS considers the following factors (IRS Publication 15-A (Employer's Supplemental Tax Guide) (available at http://www.irs.gov/pub/irs-pdf/p15a.pdf)):

- **The amount of instruction provided to the worker, including, but not limited to, when and where to do the work, what tools or equipment to use, where to purchase supplies or services, and what order or sequence to follow in accomplishing the work.** In general, evidence that a company has the right to specify only the end result of a project and not the tools, methodologies, equipment, suppliers, or sequence of work used by a worker tends to indicate that the company has an independent contractor relationship with that worker. Independent contractors tend to receive only the minimum amount of instruction needed to properly perform the task desired. Workers who are directed to use particular tools at particular locations and particular suppliers are more likely to be employees.
- **The amount of training provided to the worker to perform particular services in a particular manner.** Facts tending to show that the worker received a significant amount of training, either verbally or through manuals, concerning how to accomplish a project support the existence of an employer-employee relationship. Independent contractors are less likely to receive training to perform work in a specific way, and tend to follow their own methods.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/4 Human Resources/§4.16 2. Financial Control

§4.16 2. Financial Control

In analyzing whether a company exercises financial control over a worker, the IRS considers the following factors (IRS Publication 15-A (Employer's Supplemental Tax Guide) (available at http://www.irs.gov/pub/irs-pdf/p15a.pdf)):

- **The extent to which the worker is reimbursed for business expenses.** Employees are more likely to receive reimbursement for business expenses.
- **The extent of investment the worker has in the facilities or tools needed to complete the work.** Independent contractors tend to be workers who have invested a significant amount of money in a particular set of tools or equipment and who use those tools or operate that equipment in their own facilities.
- **The extent to which the worker makes the services performed available in the relevant market.** Independent contractors, although often restricted from working for competitors while retained by a company, are usually free to offer services to other entities. A worker who does offer services to the market in general, as well as to a particular company, is more likely to be classified as an independent contractor.
- **The method by which the individual is compensated for the work performed.** Employees tend to receive regular, guaranteed wages that are independent of the quality or amount of work (other than their time) spent on a particular project. Independent contractors tend to be compensated with flat fees or other fee arrangements that are less regular and that provide incentives to accomplish the work in as efficient a manner as possible.
- **The extent to which the worker can realize a profit or loss.** Employees typically do not profit from the success of their work on an individual project or assignment, while independent contractors may earn a profit or loss on their assignment depending on their fee arrangement, their expenses, and the amount of time it takes them to properly complete the project.

© The Regents of the University of California

§4.17 3. Type of Relationship

In considering whether a worker has an independent contractor relationship with a company, the IRS examines the following factors (IRS Publication 15-A (Employer's Supplemental Tax Guide) (available at http://www.irs.gov/pub/irs-pdf/p15a.pdf)):

- **The existence of a written contract describing the relationship.** Independent contractors are more likely to have specific written agreements describing the nature of the work to be performed and the compensation for performing the work.
- **The benefits provided to the worker.** Independent contractors do not usually receive health or life insurance, sick pay, vacation pay, or other benefits typical in an employer-employee relationship.
- **The permanency of the relationship.** Independent contractor relationships are usually for a fixed period of time, or until a particular project is completed.
- **The extent to which the services performed by the worker are a key aspect of the normal business of the company.** Independent contractors are typically hired to perform a service that is outside the scope of the normal business and operations of a company. Employees tend to perform the everyday business and operations of the company. Independent contractors may be retained in peak seasons, however, when existing employees cannot complete all the work necessary for operation of the business.

© The Regents of the University of California

§4.18 C. Intellectual Property Issues in Independent Contractor Relationships

Online businesses should ensure that software and other intellectual property created by independent contractors is properly addressed in an independent contractor agreement. In an employer-employee relationship, the work-for-hire doctrine under the Copyright Act (17 USC §201(b)) provides that the employer or other person for whom a work is prepared is generally considered the author of that work. See §4.8. The work-for-hire doctrine is discussed in more detail in §1.5.

Section 201(a) of the Copyright Act (17 USC §201(a)) states that a copyright in a work "vests initially in the author or authors of the work." Thus, without an assignment or exclusive license, a company may have no, or very limited, rights in the use of copyrights created by independent contractors. For example, assume that the company hires a programmer as an independent contractor to create a piece of software. The company then licenses the finished software product to others and generates revenue. Absent an agreement transferring title or granting a license to the code created by the programmer to the company, it is not clear the company has the right to use the software. Because the work was not created by an employee of the company, the rules that apply to works for hire may be inapplicable, and title to the work may remain with the contractor. Moreover, the company may owe royalties to the independent contractor (above and beyond the fees already paid to create the software) for licensing or using the software, or both. Finally, assuming the independent contractor does own the software product, the contractor would be free to license or sell the software to others, including the company's competition. For sample language assigning or granting an exclusive license in a copyright, see paragraph 11 of the Independent Contractor Consulting Agreement in §4.19.

Companies should seek to avoid situations in which an independent contractor does not develop an entire work, but rather simply adds intellectual property to a work jointly created with the company. Joint authors are joint owners of a copyright and have the right to share in profits. See 17 USC §201(a). Without an assignment from the independent contractor to the company, the company may have a continuing obligation to the independent contractor to share profits generated from the joint work. For sample assignment language, see paragraph 11 of the Independent Contractor Consulting Agreement in §4.19. For further discussion of copyright issues, see chap 1.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/4 Human Resources/§4.19 D. Form: Independent Contractor Consulting Agreement

§4.19 D. Form: Independent Contractor Consulting Agreement

▶ To download **Word** version, right click and choose *Save Target As*

▶ To download **WordPerfect** version, right click and choose *Save Target As*

INDEPENDENT CONTRACTOR CONSULTING AGREEMENT

This Independent Contractor Consulting Agreement (this "Agreement") is made as of _ _[*date*]_ _, between _ _[*name of company*]_ _, a _ _[*specify entity, e.g., California corporation*]_ _ ("Company"), and the person or entity identified as "Consultant" on the signature page of this Agreement ("Consultant").

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties agree as follows:

1. SERVICES. Company hereby retains Consultant to perform the following services (the "Services"): _ _[*List or describe services as specifically as possible. The services can be more specifically described in an attached exhibit if necessary.*]_ _

Comment: The description of the services should be as precise as possible and should avoid the use of general terms such as "and such other services as may be added from time to time" or "such services as directed by the appropriate employees of Company" to lessen the risk of potential reclassification of the independent contractor as an employee.

2. TERM. The term of this Agreement shall begin on the date first set forth above and shall continue until _ _[*ending date of term*]_ _ (the "Term"), unless earlier terminated as provided for herein.

Comment: The term of the agreement should be for a specified period of time, or else should end on completion of a specific project that has a reasonably certain time frame for completion. Avoid using open-ended or automatically renewing terms because permanency of the relationship is a factor for classifying a worker as an employee.

3. CONSIDERATION. As full and complete payment for all Services rendered under this Agreement, Consultant shall be compensated as follows: _ _[*describe amount to be paid, how calculated, and terms upon which payment is to be made (such as net 30 days after receipt of invoice by Company)*]_ _ **(the "Compensation").**

Comment: The IRS considers how a worker is compensated as a factor in determining whether to classify that worker as an independent contractor. See §4.16. Flat fee arrangements, which differ from regularly paid wages that are not tied to a project's completion, are more indicative of an independent contractor relationship because they are not guaranteed and give the independent contractor a chance for profit or loss. Consider providing for a bonus on completion of the project within a certain timeframe.

4. LOCATION. Consultant shall perform the Services at the following location: _ _[*address or other description of where Consultant will work*]_ _**, or such other location as the parties may mutually agree in writing (the "Location").**

Comment: Consider deleting this section if there is no compelling reason for requiring the consultant to work at the specified location, *i.e.,* if the consultant can successfully perform the services elsewhere.

5. INDEPENDENT CONTRACTOR STATUS. Consultant is an independent contractor and not a Company employee. Nothing in this Agreement creates or is intended to create any employment relationship between Consultant and Company. Consultant shall not be eligible to participate in or receive any benefit from any benefit plan or program available to Company employees. Company shall not provide workers' compensation coverage for Consultant. Consultant shall comply with all applicable laws and regulations and shall have sole responsibility for the payment of all applicable taxes and withholdings with respect to Compensation paid to Consultant. All persons employed or retained by Consultant in connection with Consultant's performance of the

Services shall be considered employees of Consultant and not of Company. Consultant retains sole and absolute discretion in the manner and means of carrying out the Services.

Comment: A company should not consider this language to be sufficient to guarantee classification as an independent contractor if the actual relationship between the company and worker differs from what is described in this agreement.

6. REPORTS. Consultant shall provide to Company periodic written reports of Consultant's activities in a manner and format acceptable to Company, and shall provide related work records, meeting reports, and similar documents as requested by Company. Consultant agrees to be available for meetings with Company employees and contractors.

7. CONSULTANT'S REPRESENTATIONS. Consultant represents and warrants that any and all information, practices, or techniques to be described, demonstrated, divulged, or made known to Company during the performance of the Services may be divulged without any obligation to, or violation of any right of, others. Consultant further represents and warrants that any and all practices or techniques that Consultant shall disclose, along with any related materials, may be freely used by Company without violation of any law or payment of any royalty, except as Consultant shall specifically identify in writing, subject to Company's right to approve, in its discretion, the use of any such materials.

8. CONFIDENTIALITY. To govern the exchange of any and all confidential, proprietary, and other similarly sensitive information, the parties shall execute and be bound by the terms of the nondisclosure agreement attached hereto as Exhibit _ _.

Comment: See §4.21 for a form of independent contractor nondisclosure agreement.

9. OTHER EMPLOYMENT. During the Term, Consultant shall not, without the prior written consent of Company, (a) enter into or engage in any business that competes with the business of Company, or (b) promote or assist, financially or otherwise, or invest in any person, firm, association, partnership, corporation, or other entity engaged in any business that competes with the business of Company, except for passive investments of less than 5% in publicly traded companies.

Comment: Note that this provision does not prevent the independent contractor from seeking other work. If the services performed by the independent contractor are applicable to only one type of business (*e.g.,* software programming), consider a restriction that only applies to a subset of that business (*e.g.,* development of gaming software), so as to not overly restrict the independent contractor's ability to engage in other work.

[*If appropriate, add*]

Unless earlier terminated as provided in this Agreement, during the Term, Consultant shall devote at least _ _[*number*]**_ _ hours per week to the completion of the Services until the Services are completed.**

Comment: If the type or amount of services warrants, consider specifying the amount of time that the independent contractor will be required to devote to the services.

[*Continue*]

10. NO SOLICITATION. During the Term and for a period of _ _[*e.g., one (1) year*]**_ _ following the expiration or earlier termination of this Agreement, Consultant shall not directly or indirectly solicit or induce or attempt to solicit or induce any customer, vendor, employee, sales representative, agent, or consultant of Company to terminate or adversely alter their employment, representation, or other association with Company.**

11. ASSIGNMENT OF RIGHTS. Consultant hereby assigns and agrees to assign to Company all of Consultant's rights to any of the following, whether made, conceived, or suggested, either alone or jointly with others, by Consultant while engaged by Company, whether in the course of Consultant's engagement, or with the use of Company's time, material, or facilities, or in any way within or related to the existing or contemplated scope of Company's business: (a) work papers, reports, documentation, drawings, photographs, negatives, tapes and masters for tapes, prototypes, and other materials (the "Items"), including without limitation any and all such Items generated and maintained on any form of electronic media, generated by Consultant during the Term; and (b) discoveries, inventions, and improvements (the "Inventions"), whether patentable or not. Any Item or Invention directly derivative of Company's planned or existing products or services, developed or under

development during Consultant's engagement, and made, conceived, or suggested by Consultant, either alone or jointly with others, within _ _[*e.g., one (1) year*]_ _ following termination of Consultant's engagement under this Agreement or any successor agreements, shall be irrebuttably presumed to have been made, conceived, or suggested in the course of Consultant's engagement and with the use of Company's time, materials, or facilities.

Consultant's initials _____

Comment: See §§4.6-4.11 for discussion of invention assignment agreements between employers and employees. Consider requesting the independent contractor to initial this section as acknowledgement of the assignment.

12. DISCLOSURE OF AGREEMENT. During the Term of this Agreement and for _ _[*e.g., one (1) year*]_ _ after its expiration or earlier termination, Consultant shall communicate the contents of Paragraphs 8 (Confidentiality), 10 (No Solicitation), and 11 (Assignment of Rights) of this Agreement to any person or entity that intends to employ, associate with, or be represented by Consultant and that is engaged in a business that is competitive to the business of Company.

13. REMEDIES. Consultant acknowledges that the actual or threatened disclosure of Confidential Information (as such term is defined in the Mutual Nondisclosure Agreement of even date herewith between Consultant and Company) or any breach of the provisions of Paragraph 8, 9, 10, or 11 of this Agreement may give rise to irreparable injury to Company that cannot be adequately compensated with monetary damages. Consultant agrees that Company may seek and obtain injunctive relief against the breach or threatened breach of any of those provisions or specific enforcement of those provisions in addition to any other legal or equitable remedies that may be available.

14. INDEMNIFICATION. Consultant shall indemnify, defend, and hold harmless Company from and against any and all losses, claims, and expenses (including reasonable attorney fees) directly or indirectly arising out of or resulting from (a) any act or omission of Consultant related to services performed for Company under this Agreement; (b) any unauthorized use by Consultant of Confidential Information; or (c) any breach of any representation, warranty, or covenant of Consultant contained in this Agreement, or otherwise made to Company.

15. NO ASSIGNMENT. Consultant shall not assign or subcontract any right in or obligation arising under this Agreement without Company's prior written consent. Any assignment in violation of this paragraph shall be void. This Agreement shall be binding on and inure to the benefit of each party's heirs, executors, legal representatives, successors, and permitted assigns.

Comment: If the consultant has a specific set of unique skills and has been engaged based on its own expertise, a clause prohibiting assignment will protect against a transfer of the agreement by the consultant to a third party but will not protect against the consultant hiring subcontractors or temporary help to work on the project. Consider adding a statement that the consultant may not subcontract the work or that the contractor must use certain designated employees to complete the work.

16. TERMINATION. Either party may terminate this Agreement at any time with or without cause on not less than thirty (30) days' prior written notice to the other party. In the event of termination, Company shall not be liable to Consultant for compensation or damages of any kind whatsoever, including direct, incidental, or consequential damages, incurred as a result of such termination, other than Compensation payable under this Agreement for Services performed before termination.

17. NOTICES. Whenever notice is to be served under this Agreement, service shall be made personally, by facsimile transmission, by overnight courier, or by registered or certified mail, return receipt requested. Notice shall be effective only on receipt by the party being served, except notice shall be deemed received 72 hours after posting by the United States Post Office in the manner described in this paragraph.

18. FURTHER ASSURANCES. From time to time, each party shall execute and deliver such instruments as maybe reasonably necessary to carry out the purposes and intent of this Agreement. In addition, Consultant shall promptly disclose all Inventions to Company and shall perform all acts necessary or desirable to assist Company, at its expense, in obtaining and enforcing the full benefits, enjoyment, rights, and title in and to the Inventions throughout the world.

19. SURVIVAL. The provisions of Paragraphs 3, 8, 10, 11, 12, 13, 14, 17, 18, 19, and 20, as well as any other terms of this Agreement that expressly extend or by their nature should extend beyond termination or expiration of this Agreement, shall survive and continue in full force and effect after any termination or expiration of this Agreement.

20. GOVERNING LAW. This Agreement shall be governed by California law, without reference to rules regarding conflicts of law.

21. COUNTERPARTS. This Agreement may be executed in multiple counterparts, each of which shall constitute an original and all of which together shall constitute one instrument.

22. SEVERABILITY. If any term or provision of this Agreement, or the application thereof to any person or circumstance, shall to any extent be found to be invalid, void, or unenforceable, the remaining provisions of this Agreement and any application thereof shall, nevertheless, continue in full force and effect without being impaired or invalidated in any way.

23. WAIVER. No waiver of any term, provision, or condition of this Agreement, whether by conduct or otherwise, in any one or more instances, shall be deemed to be or be construed as a further or continuing waiver of any such term, provision, or condition or as a waiver of any other term, provision, or condition of this Agreement.

24. ENTIRE AGREEMENT. This Agreement, along with its exhibits, contains the entire agreement and understanding of the parties with respect to the subject matter of this Agreement, and merges and supersedes all prior agreements, discussions, and writings with respect to that subject matter. No modification or alteration of this Agreement shall be effective unless made in writing and signed by both Consultant and Company.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the first day above written.

COMPANY

Date: _ _ _ _ _ _

_ _[*NAME OF COMPANY*]_ _,
a _ _[*state of incorporation*]_ _ **corporation**

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

Company's Address:

_____
_____
_____
Phone: _____
Fax: _____

CONSULTANT

Date: _ _ _ _ _ _

__[*Signature*]__
_ _[*Typed name of Consultant*]_ _

Consultant's Address:

_____
_____
_____
Phone: _____
Fax: _____

Social Security Number: _____

© The Regents of the University of California

E. Independent Contractor Nondisclosure Agreement

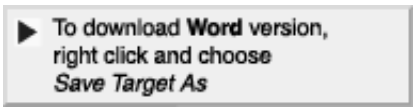
§4.20 1. Introduction

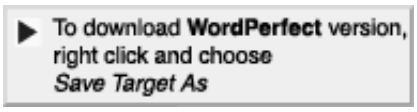
The form of nondisclosure agreement in §4.21 is designed to be used in tandem with the Independent Contractor Consulting Agreement provided in §4.19.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/4 Human Resources/§4.21 2. Form: Nondisclosure Agreement

§4.21 2. Form: Nondisclosure Agreement





NONDISCLOSURE AGREEMENT

This Nondisclosure Agreement (the "Agreement") is entered into as of _ _[*date*]_ _ (the "Effective Date"), between _ _[*name of company*]_ _ (the "Company") and _ _[*name of independent contractor*]_ _ (the "Contractor") (collectively, the "Parties" and each a "Party").

WHEREAS, the Company has certain confidential information relating to its business that it desires to disclose to Contractor for purposes of the performance of that certain Independent Contractor Consulting Agreement dated _ _[*date*]_ _ (the "Project").

NOW THEREFORE, in consideration of the covenants and agreements contained herein and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. CONFIDENTIAL INFORMATION. Except as provided in Section 2, as used in this Agreement, "Confidential Information" means any information furnished or disclosed, in whatever form or medium, by the Company to the Contractor relating to the business of the Company, and includes, without limitation, contract terms, financial information, business procedures, processes, techniques, methods, ideas, discoveries, inventions, developments, records, product designs, source codes, product planning, trade secrets, customer lists, and material samples, all of which is deemed confidential and proprietary.

Comment: If any additional items would be relevant as confidential information, they should be included in this definition. If the fact that the parties are engaged in the project should be confidential, this should be added. If any other agreement between the parties is confidential, it should be added to this list.

2. EXCLUSIONS FROM DEFINITION OF CONFIDENTIAL INFORMATION. Notwithstanding any other provision of this Agreement, each Party acknowledges that Confidential Information does not include any information that the Contractor can demonstrate (a) was publicly available at the time of disclosure, or later became publicly available through no act or omission of the Contractor; (b) was already in the Contractor's possession at the time of disclosure; (c) was rightfully received by the Contractor from a third party without any obligation of confidentiality; or (d) was independently developed by or for the Contractor without use of the Confidential Information.

[*If appropriate, add*]

The residuals resulting from access to the Confidential Information or from work with Company shall not be subject to the confidentiality obligations contained in this Agreement. The term "residuals" means information in nontangible form that may be retained in the unaided memories of persons who have had access to the Confidential Information, including ideas, concepts, know-how, or techniques contained therein. Contractor shall have no obligation to limit or restrict the assignment of such persons or to pay royalties for any work resulting from the use of residuals.

Comment: A sophisticated contractor may require the inclusion of a residuals clause similar to the one above to preserve the contractor's knowledge base. Consultants build their knowledge base through varied jobs. This clause permits their future use of general skills they learn during the course of this engagement. This type of provision, however, is a loophole that dilutes the strength of the agreement. If the principal idea is obvious and easy to remember (an "aha"), this kind of clause poses a problem. If the company has a strong patent position, or the idea is inherently complex and not susceptible to unaided memorization, this clause may be less problematic.

[*Continue*]

3. USE OF CONFIDENTIAL INFORMATION. The Contractor shall use the Confidential Information only for the purpose of the Project, and shall make no use of the Confidential Information, in whole or in part, for any other purpose. The Contractor agrees to refrain from disclosing the Confidential Information to third Parties, unless the Company has given its prior written authorization. The Contractor further agrees to keep confidential all of the Confidential Information and to take all reasonable steps to preserve the confidential and proprietary nature of the Confidential Information.

Comment: Depending on the nature of the project, consider restricting the removal of the confidential information from a central location or computer.

4. REQUIRED DISCLOSURE. If the Contractor is requested or required by subpoena or other court order to disclose any of the Confidential Information, the Contractor shall provide immediate notice of such request to the Company and shall use reasonable efforts to resist disclosure, until an appropriate protective order may be sought, or a waiver of compliance with the provisions of this Agreement granted. If, in the absence of a protective order or the receipt of a waiver under this Agreement, the Contractor is nonetheless, in the written opinion of its counsel, legally required to disclose any Confidential Information, then, in such event, the Contractor may disclose such information without liability under this Agreement, provided that the Company has been given a reasonable opportunity to review the text of such disclosure before it is made and that the disclosure is limited to only the Confidential Information specifically required to be disclosed.

5. RETURN OF CONFIDENTIAL INFORMATION. The Company may elect at any time to terminate further access to its Confidential Information. On written request, the Contractor shall return to the Company all Confidential Information in any form and promptly destroy any and all material or information derived from the Confidential Information, including any copies, except that one copy of the same may be retained for archival and evidence purposes only.

6. NO OWNERSHIP OR OTHER RIGHTS GRANTED. Nothing contained in this Agreement shall be construed as granting or conferring any rights, by license or otherwise, express or implied, in or to any patents, copyrights, trademarks, know-how, or other proprietary rights of either Party acquired before or after the date of this Agreement.

7. TERM. This Agreement and the obligations of confidentiality and nondisclosure contained in it shall remain in full force and effect for the period that is the greater of (a) the term of Independent Contractor Consulting Agreement plus _ _[*number*]_ _ years; (b) _ _[*number*]_ _ years after the Effective Date; or (c) such longer time as the Parties may agree in writing.

8. REMEDIES FOR BREACH OF AGREEMENT. The Confidential Information protected by this Agreement is of a special character, such that money damages would not be sufficient to award or compensate for any unauthorized use or disclosure of the Confidential Information. The Parties agree that injunctive and other equitable relief would be appropriate to prevent any such actual or threatened unauthorized use or disclosure. The remedies stated above may be pursued in addition to any other remedies available at law or in equity, and the Contractor agrees to waive any requirement for the securing or posting of any bond in connection with such remedies. In the event of litigation to enforce any provision of this Agreement, the prevailing Party shall be entitled to recover all costs, including its reasonable attorney fees and costs, incurred in connection with the litigation.

9. NO OTHER AGREEMENT. This Agreement is not and shall not be construed as any form of a letter of intent or agreement to enter into any type of transaction. This Agreement is to evidence the Parties' agreement to maintain the confidentiality of the Confidential Information, and shall not constitute any commitment or obligation on the part of either Party to enter into any specific contractual arrangement of any nature whatsoever.

10. NO REPRESENTATIONS. The Company does not make any representations or warranties as to the accuracy, completeness, or fitness for a particular purpose of any information disclosed to the Contractor under this Agreement. Neither the Company nor its representatives shall have any liability or responsibility to the Contractor (except as provided in this Agreement) or to any other person or entity resulting from the use of any information so furnished or otherwise provided.

11. GOVERNING LAW. California law shall govern the interpretation of this Agreement, without reference to rules regarding conflicts of law. Any dispute arising out of this Agreement shall be submitted to a state or

federal court sitting in California, which shall have the exclusive jurisdiction regarding the dispute and to whose jurisdiction the Parties irrevocably submit.

12. NO WAIVER. No waiver of any term, provision, or condition of this Agreement, whether by conduct or otherwise, in any one or more instances, shall be deemed to be or be construed as a further or continuing waiver of any such term, provision, or condition or as a waiver of any other term, provision, or condition of this Agreement.

13. SEVERABILITY. If any provision of this Agreement is determined by any court of competent jurisdiction to be invalid or unenforceable, such provision shall be interpreted to the maximum extent to which it is valid and enforceable, all as determined by such court in such action, and the remaining provisions of this Agreement shall, nevertheless, continue in full force and effect without being impaired or invalidated in any way.

14. ENTIRE AGREEMENT. This Agreement constitutes the Parties' entire Agreement with respect to the subject matter hereof and supersedes any and all prior statements or agreements, both written and oral. This Agreement may not be amended except by a writing signed by the Parties.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed by their duly authorized representatives.

COMPANY

Date: _ _ _ _ _ _

_ _[*NAME OF COMPANY*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

Company's Address:

_____
_____
_____
Phone: _____
Fax: _____

CONSULTANT

Date: _ _ _ _ _ _

__[*Signature*]__
_ _[*Typed name of Consultant*]_ _

Consultant's Address:

_____
_____
_____
Phone: _____
Fax: _____

Social Security Number: _____

© The Regents of the University of California

III. ADVISORY BOARDS

§4.22 A. Introduction

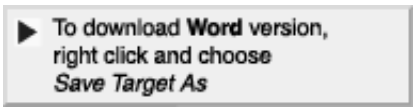
Companies operating in technology sectors often name a panel of experts in the company's industry to sit on a board of advisors for the company. Advisors may help the company formulate corporate strategy, identify strategic partners, form alliances, find financing, and develop future products. Companies may pay advisors a salary plus expenses. Frequently, in addition to or in place of a salary, advisors receive options to purchase shares of the company's capital stock.

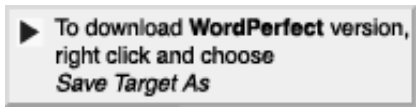
Companies should officially engage an advisor through a letter agreement that delineates the expectations and role for the advisor, confidentiality requirements, and any compensation the advisor is to receive. A model form of Advisory Board Letter Agreement for a start-up business is provided in §4.23. Counsel should consider whether to have advisory board members also sign a separate confidentiality agreement.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/4 Human Resources/§4.23 B. Form: Advisory Board Letter Agreement

§4.23 B. Form: Advisory Board Letter Agreement





[*Company letterhead*]

_ _[*Date*]_ _

_ _[*Advisor's name and address*]_ _

Dear _ _[*advisor's name*]_ _,

On behalf of _ _[*name of company*]_ _ (the "Company"), thank you for agreeing to serve on the Company's Advisory Board (the "Advisory Board"). We are very pleased to welcome you as part of our team. This letter will serve as our agreement regarding your participation on the Advisory Board. Please counter-sign where indicated below to confirm your agreement to the following points of understanding.

1. YOUR SERVICES AS ADVISORY BOARD MEMBER. You will be serving as a member of the Advisory Board along with other members worldwide. Your services will include participation in quarterly formal meetings of the Advisory Board, which is expected to convene from time to time by audio/video conference call, as well as consultation with Company personnel by phone and e-mail from time to time as the need arises. As a general matter, your responsibilities will include:

Providing strategic guidance and direction to the Company;

Providing introductions to possible strategic partners and sources of investor funding, and participating, to the extent possible, in meetings between the Company and such individuals or entities; and

Contributing your own ideas and information about the development of products and services for the Company.

In performing your services under this agreement and in providing advice and review, we expect you to use your reasonable best efforts and judgment. We welcome your input on business and operational matters related to the Company.

2. COMPENSATION. In consideration for your services, and the other duties set forth in this agreement, you will receive the following:

(a) An advisory board fee of _ _[*dollar amount*]_ _ per _ _[*meeting attended/quarter*]_ _, payable within 30 days after the end of each calendar quarter you serve on the advisory board _ _[*, prorated for partial quarters*]_ _.

(b) Options to purchase up to _ _[*number of shares*]_ _ shares of common stock in the Company (the Options). The Options will be granted on the same terms available to employees of the Company under its equity participation plan. The Options will vest over _ _[*number of years*]_ _ years in monthly installments for as long as this agreement remains in effect and you continue to serve on the Advisory Board. You will have _ _[*number of years*]_ _ years from the date of this letter to exercise the Options, and the exercise price will equal the fair market value on the date of this letter, as determined by the Company's board of directors in its sole discretion. On the termination of this agreement for any reason, no further shares will vest, but you will remain entitled to exercise those Options that vested on or before the effective date of termination. The Options granted under this agreement represent your total consideration for service as a member of the Advisory Board, notwithstanding the fact that this agreement may be renewed in accordance with Paragraph 4 below.

3. EXPENSES. The Company will reimburse you for your reasonable, documented expenses incurred in

connection with your membership on the Advisory Board, including costs of photocopying, mailing, and supplies. You agree to obtain the prior written approval of the Company before incurring any expenses in excess of _ _[*dollar amount*]_ _ per month.

4. TERM. Your term as a member of the Advisory Board will be _ _[*e.g., one year*]_ _ from the date of your signature on this agreement. This term will automatically renew for successive _ _[*e.g., one-year*]_ _ periods, unless either party provides the other party with written notice of its intent not to renew at least thirty (30) days before the end of the then-current term.

5. USE OF NAME, IMAGE, AND BIOGRAPHICAL DATA. You agree that the Company may identify you as a member of the Advisory Board, and from time to time use your biographical data and profile in connection with the Company's promotional efforts.

6. EXCLUSIVITY. During the term of this agreement, and as otherwise agreed in writing by you and the Company, you agree not to render comparable services for, or otherwise participate in the business of, any person or company that competes with the Company in _ _[*describe Company's business*]_ _, except with the prior written consent of the Company.

7. NONDISCLOSURE. During your term as a member of the Advisory Board, you may be asked to review confidential and proprietary information and materials, including information and materials protected under trade secret, copyright, trademark, patent, and other intellectual property laws. You agree to hold all such information and materials in confidence, you agree not to disclose any such information and materials to any other person or entity for any purpose, and you agree not to use any such information or materials in competition with the Company. At the end of your term, you agree to return to the Company all copies of such information and materials.

8. NO EMPLOYMENT OR OTHER RELATIONSHIP. This letter is an arm's-length agreement between independently contracting parties. Except as expressly provided in this agreement, no employment, trust, agency, joint authorship, or other legal relationship is created between you and the Company. You are not an agent of the Company and you are not authorized to enter into contracts or make any representations and commitments on behalf of the Company.

9. OWNERSHIP OF INTELLECTUAL PROPERTY. We do not expect you to create works of authorship or other intellectual property solely in connection with your service as a member of the Advisory Board. You agree, however, to promptly and fully disclose any intellectual property that you may incidentally create or contribute as part of your participation in formal meetings of the Advisory Board. You also agree that all such intellectual property will belong to the Company, and you hereby assign and agree to assign such rights to the Company.

10. ASSURANCES. You assure the Company that, to the best of your knowledge, there is no restriction on your entering into this agreement. You acknowledge that the exclusivity and noncompetition provisions in Paragraphs 6 and 7 will remain in effect for one year after the expiration or earlier termination of this agreement. You also acknowledge that your obligation not to disclose the confidential and proprietary information of the Company as described in Paragraph 7 will survive the expiration or earlier termination of this agreement.

11. EARLY TERMINATION. We are entitled to remove you from the Advisory Board before the expiration of the term of this agreement for any reason on written notice to you.

Please confirm your agreement by initialing where indicated above, signing where indicated below, and return the counter-signed letter to the Company. We are looking forward to welcoming you to the Advisory Board and working with you.

Sincerely yours,

Date: _ _ _ _ _ _

_ _[*NAME OF COMPANY*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ __

Its: _ _[*Title*]_ _

Agreed and accepted:

Date: _ _ _ _ _ _ __[*Signature*]__
_ _[*Typed name of advisor*]_ _

© The Regents of the University of California

5

Website Development

I. ACQUISITION OF INTELLECTUAL PROPERTY
- A. Introduction §5.1
- B. Assignment of Intellectual Property by Company Founder §5.2
- C. Form: Agreement for Transfer and Assignment of Intellectual Property §5.3

II. WEBSITE DEVELOPMENT AGREEMENTS
- A. Introduction §5.4
- B. Ethical Considerations §5.5
- C. Preparing for Negotiations §5.6
- D. Types of Website Developers §5.7
  - 1. Freelancers §5.8
  - 2. Website Development Specialists §5.9
  - 3. General Technology Companies §5.10
- E. Understanding Issues of Ownership
  - 1. Conflicting Ownership Interests §5.11
  - 2. Why a Website Probably Is Not a "Work Made for Hire" §5.12
  - 3. Domain Name Registration and Ownership §5.13
- F. Drafting Website Development Agreement §5.14
  - 1. Responsibilities of Parties §5.15
  - 2. Deliverables and Timelines for Delivery §5.16
  - 3. Ownership and License Grants §5.17
    - a. Ownership §5.18
    - b. License Rights §5.19
    - c. Confidentiality §5.20
  - 4. Representations and Warranties of Developer §5.21
  - 5. Ongoing Obligations of Developer §5.22
- G. Website Development Agreements
  - 1. Independent Contractor Agreements §5.23
  - 2. Form of Website Development Agreement
    - a. Introduction §5.24
    - b. Form: Website Development Agreement §5.25
- H. Upgrading Website §5.26

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/5 Website Development/ I. ACQUISITION OF INTELLECTUAL PROPERTY/§5.1 A. Introduction

I. ACQUISITION OF INTELLECTUAL PROPERTY

§5.1 A. Introduction

Intellectual property rights—copyrights, trademarks, service marks, domain names, trade secrets, and patents—are the foundation of many (if not all) online businesses, and, with the growth of the Internet and the World Wide Web, have assumed central importance for "bricks and mortar" companies as well. For any business with a substantial online presence, intellectual property rights and the technology embodying those rights provide much of the value inherent in the business's Internet website. These intangible assets may be created by the founders of the company, independent contractors, or employees of the company. Alternatively, intellectual property rights may be acquired through the purchase of another business, a division, or a website, or by direct purchase of the rights themselves. Intellectual property rights generally vest in the author or creator of the work. See §§4.6-4.8. Thus, a threshold question is what person or entity is the owner of the rights.

EXAMPLE: The founder of a company obtains a patent in the founder's name for a new process that the founder invented, then forms a corporation specifically for the purposes of utilizing the patent to provide goods or services. The company is not the owner of the patent until the founder assigns the patent to the company, usually in exchange for equity or debt securities in the company.

An attorney advising an online business in connection with its early growth or overseeing the development of a company's Internet website should inventory the intellectual property needed for the website and the company's other operations, determine its ownership, and also determine whether or not the intellectual property is registered with the United States Patent and Trademark Office (USPTO) or the United States Copyright Office. If an assignment of the intellectual property will be required to transfer ownership to the company, the formalities vary depending on what type of intellectual property is involved and whether or not the intellectual property has been registered at the federal level. Counsel should consult applicable statutes and regulations to determine the appropriate transfer procedures.

In general, assignments of intellectual property must be in writing, either under the federal or state laws regulating the particular type of intellectual property involved (see 35 USC §261 and §§2.15-2.17 (patents); 17 USC §204 and §§1.9-1.11 (registered copyrights); 15 USC §1060 and §§3.57-3.59 (federally registered trademarks); Bus & P C §14220 (state registered trademarks)), or under the state Statute of Frauds (CC §1624). See also §§3.7-3.8, 22.18-22.19 (domain names). Counsel should note that assignments of trademarks are not valid unless accompanied by an assignment of the goodwill of the business in which the mark is used or of that part of the goodwill of the business associated with the mark. See 15 USC §1060(a); §3.57. To be effective against bona fide purchasers for value without notice of the assignment, assignments of federal or state registered intellectual property must be recorded in the applicable federal or state office, in accordance with applicable statutory procedures. See 35 USC §261 and §§2.15-2.17 (patents); 17 USC §205 and §§1.9-1.11 (registered copyrights); 15 USC §1060 and §§3.57-3.59 (federally registered trademarks); Bus & P C §14260 (state registered trademarks). See also §§3.7-3.8, 22.18-22.19 (domain names).

Whenever possible, all rights in the intellectual property used or intended to be used by the company should be assigned outright to the company. A form of an assignment agreement is provided in §5.3. If assignment of all rights is not possible, the company should seek an exclusive license for its use of the rights, but counsel should bear in mind that investors tend to disfavor companies that do not own their core intellectual property outright. If an exclusive license is the only way that key intellectual property can be acquired, counsel should consult chap 11 on license agreements. The license should be drafted to cover all possible lines of business that the company might engage in, and should remain in effect for as long as possible.

The enterprise value of a company depends not only on the value of assets that the company owns outright but also on the value of its rights to use assets under licensing or other collaborative arrangements. Intellectual property ownership issues should be considered carefully throughout all phases of growth of an online business, and particularly when development of a website is proposed or undertaken.

© The Regents of the University of California

§5.2 B. Assignment of Intellectual Property by Company Founder

The form in §5.3 represents a simple assignment of intellectual property to be used in connection with a founder's contribution of patents, copyrights, trademarks, or trade secrets to a new company. For example, if the founder has prepared a business plan and a partially working basic demonstration model of a website, the copyright in the business plan, the ideas and concepts giving rise to that plan, the trademark in the name of the business (to the extent used by the founders before incorporation), and all intellectual property rights in the website model should be transferred to the company. Alternatively, these rights or a portion of them may be licensed exclusively to the company on a royalty-bearing or royalty-free basis. When a company plans to seek outside financing, however, the founders usually transfer ownership of all intellectual property rights to the company, to increase the company's enterprise value. For forms of assignment addressed to specific types of intellectual property, see §§2.15-2.17 (patents); §§1.9-1.11 (registered copyrights); §§3.57-3.59 (federally registered trademarks); and §§3.7-3.8, 22.18-22.19 (domain names).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/5 Website Development/§5.3 C. Form: Agreement for Transfer and Assignment of Intellectual Property

§5.3 C. Form: Agreement for Transfer and Assignment of Intellectual Property

▶ To download **Word** version, right click and choose *Save Target As*

▶ To download **WordPerfect** version, right click and choose *Save Target As*

TRANSFER AND ASSIGNMENT OF INTELLECTUAL PROPERTY

This Agreement for Transfer and Assignment of Intellectual Property (the Agreement) is made and entered into as of _ _[*effective date*]_ _**, between** _ _[*name of assignor*]_ _ **("Assignor") and** _ _[*name of assignee*]_ _ **("Assignee").**

1. DESCRIPTION OF INTELLECTUAL PROPERTY. Assignor is the owner of the following items of intellectual property (the "Intellectual Property): _ _[*Insert identifying information such as title, registration number for patents, trademarks, or copyrights, description of trade secrets*]_ _**.**

2. TRANSFER AND ASSIGNMENT. For good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, _ _[*state any other consideration*]_ _**, Assignor hereby assigns and transfers to Assignee all of Assignor's interest in the Intellectual Property, together with all rights to secure registrations, renewals, reissues, and extensions of the copyrights, patents, and trademark rights included therein, if any.**

3. WARRANTIES AND REPRESENTATIONS. Assignor hereby covenants, warrants, and represents to Assignee that:

(a) Assignor is the sole owner of and has the exclusive right to use the Intellectual Property, free and clear of any liens, encumbrances, licenses, or claims of any nature, and has made no agreement with respect to the Intellectual Property that is in conflict with this Agreement.

(b) Except as specified in Paragraph 1 of this Agreement, no other registration has been effected or is on file with the appropriate governmental agencies with respect to the Intellectual Property.

(c) If Assignor is an individual, Assignor agrees to authorize and direct his or her heirs and personal representatives to make and execute any instrument and perform any legal act that Assignee may deem necessary to secure the registration, or any renewal or extension to the registration, of the Intellectual Property, as applicable.

4. GOVERNING LAW. This Agreement is governed by the laws of the State of California, without regard to conflicts of law rules.

5. ENTIRE AGREEMENT. This Agreement is the entire agreement of the parties with respect to the subject matter hereof and may not be modified or amended without the written agreement of the parties.

IN WITNESS WHEREOF, the parties have executed this Agreement by their duly authorized representatives.

Date: _ _ _ _ _ _

_ _[*NAME OF ASSIGNEE*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _
_ _[*Assignee's address*]_ _

Date: _ _ _ _ _ _

__[*Signature*]__
_ _[*Typed name of Assignor*]_ _
_ _[*Assignor's address*]_ _

© The Regents of the University of California

II. WEBSITE DEVELOPMENT AGREEMENTS

§5.4 A. Introduction

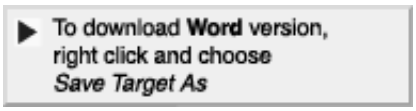
The demand for website development services has fallen off its peak from the late 1990s, resulting in a flood of available website development talent. Thus, it has become increasingly economical for businesses to engage independent website developers for their development needs. Business for developers remains brisk, because the turn away from pure Internet business models has been offset to a large degree by the number of "bricks-and-mortar" businesses that have added a website to establish an online presence, whether simply for marketing purposes or for more interactive uses, such as e-commerce or information gathering and exchange.

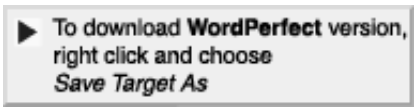
Sections 5.5-5.23 address some of the basic concerns that should guide a company in creating or obtaining development services for its website, whether those services are to be provided by company employees or, as is more common, by a third party developer. A model form of software development agreement is in §5.25. Section 5.26 discusses upgrades to existing websites and some of the issues companies may face when engaging a new developer to work on a preexisting website.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/5 Website Development/§5.5 B. Ethical Considerations

§5.5 B. Ethical Considerations





In negotiating and drafting a website development agreement for a business client, an attorney may find that the other party is a small website development shop or a freelance website developer not represented by counsel. If the opposing party is not represented, the attorney's negotiations and dealings with that party should be guided by ABA Model Rule 4.3, which provides:

> In dealing on behalf of a client with a person who is not represented by counsel, a lawyer shall not state or imply that the lawyer is disinterested. When the lawyer knows or reasonably should know that the unrepresented person misunderstands the lawyer's role in the matter, the lawyer shall make reasonable efforts to correct the misunderstanding.

Counsel representing a business in negotiations against an unrepresented website developer must be careful not to be viewed as giving any legal advice to the website developer. See generally Cal Rules of Prof Cond 3-600. Counsel should avoid having any direct dealings with the developer, communicating only with the client and letting the client relay necessary questions and information to the developer. Recognizing that this may not always be possible, however, counsel should take steps to minimize direct communications with an unrepresented developer and should avoid giving any advice to, or answering any questions about the website development agreement for, the developer.

Counsel drafting an agreement against an unrepresented party should consider including language such as the following:

Each party agrees that it has reviewed and revised this Agreement and all related documents with its counsel and that any rule of construction to the effect that ambiguities are to be construed against the drafting party shall not apply to the interpretation of this Agreement or any related document or any amendment hereto or thereto or exhibits herein or therein.

This language may not prevent a court from construing any ambiguous language in the agreement against the drafter and in favor of an unrepresented party, but it may be enough to convince the unrepresented party of the importance of consulting counsel. Many an unrepresented party has relented at the end of a negotiation and sought at least some input from counsel before executing an agreement. The unrepresented party should recognize that involving an attorney at an early point in the relationship should cost less than litigation over a dispute later on that might have been avoided.

© The Regents of the University of California

§5.6 C. Preparing for Negotiations

The importance of a written website development agreement cannot be overestimated, for purposes of both timely performance of the agreement and allocation of ownership rights in any resulting work product. Without an agreement that addresses ownership of intellectual property created by a third party developer, the presumption is that the developer, as its creator, owns all such intellectual property. See 17 USC §201(a); §§1.5, 4.8-4.9.

Website development should not be an open-ended process. In negotiating a website development agreement, a business must have a well-defined concept of how the website will look and what it will do. This concept will help not only the business itself and the website developer, but also the attorneys, who will be called on to craft an agreement that accurately reflects the ways in which the website will be developed and the site, once completed, will operate.

An attorney preparing to negotiate or draft a website development agreement should work with the client to learn the expected budget for website development, the timeframe for development, the client's understanding of the process for reviewing and approving (or rejecting) work product delivered by the website developer, and the client's understanding of who will own whatever is created. Armed with this information, the client and the attorney will be in a position to negotiate for a website that can be delivered in a timely fashion, within budget, to the client's satisfaction.

© The Regents of the University of California

§5.7 D. Types of Website Developers

In preparing to negotiate or draft a website development agreement, counsel should take into account the type of developer who will be performing services. Website development is a skill shared by many, from individuals performing services on a freelance basis, to companies whose sole business is the creation, operation, and maintenance of websites for clients, to large public companies who offer website development as just one of a wide range of technology and marketing services. By understanding the type of developer the company will be engaging, counsel is more likely to prepare a first draft of a development agreement in line with the parties' expectations and needs.

© The Regents of the University of California

§5.8 1. Freelancers

Freelancers abound in the world of website development. By keeping overhead low and working either for themselves or for small companies, freelancers are often able to offer development services at reasonable rates. For contracts with freelance developers, the parties may be able to utilize a relatively simple form of independent contractor agreement, discussed in §5.23 and in greater detail in §§4.13-4.21. The relative simplicity of the model form agreement, however, should not prevent the drafter from addressing the issues discussed in §§5.14-5.22 to help ensure that the company obtains the website it wants within the expected budget. One advantage to working with a freelancer is that the client may have more leverage in negotiations and may be able to demand greater ownership rights or other more favorable terms than in negotiations with a larger company.

© The Regents of the University of California

§5.9 2. Website Development Specialists

Website development specialists range from small development boutiques focusing on a particular industry or region to large national (or even global) companies. These specialists tend to command high prices for their services, but are in a position to offer a range of related services (such as hosting and perhaps e-commerce) once the development work has been completed. Specialists who operate in particular industries may be in the best position to accommodate a client's needs for special website features. On the other hand, these specialists probably also work with some of the company's competitors, and the company's competitive advantage may depend in part on keeping attractive and innovative features of its website designed in connection with the site's development out of its competitors' hands.

© The Regents of the University of California

§5.10 3. General Technology Companies

Many general technology companies continue to offer website development services as one of their many services through a division or subsidiary company. Expect to pay top dollar for their development services, but there is a potential advantage in dealing with a one-stop-shop if the client has other technology needs, whether or not specifically related to the website itself. In addition to hosting and technical support, these companies may provide access to custom software development services, support for electronic commerce, and perhaps even favorable hardware acquisition or leasing terms. For any large-scale website deployment, as well as for any website deployment that might be crucial to a company's business model, the services offered by a general technology company should be considered.

© The Regents of the University of California

E. Understanding Issues of Ownership

§5.11 1. Conflicting Ownership Interests

A difficult tension underlies website development agreements: Most businesses want as unique and distinctive a website as possible, while website developers typically want to reuse as much of their work product as possible on future projects. It may be helpful to resolve the issue of ownership in terms of pricing: How much would a company be willing to pay for ownership rights to its entire website, and under what circumstances would the company be willing to pay less in exchange for allowing the developer the right to reuse certain materials?

© The Regents of the University of California

§5.12 2. Why a Website Probably Is Not a "Work Made for Hire"

The doctrine of "work made for hire" is an aspect of the federal copyright law. Under 17 USC §101, there are two broad categories of works made for hire: (a) works made by employees within the scope of their employment, and (b) certain works that are "specially commissioned" when the parties expressly agree in a written agreement that the work will be considered a work made for hire. For further discussion of the doctrine of works made for hire, see §§1.5, 4.8-4.9. Although no court appears to have squarely addressed this issue, it is not clear that a website would qualify as the kind of work that can be specially commissioned to be done as a work made for hire. See generally *iXL, Inc. v AdOutlet.com, Inc.* (ED Ill 2001) 2001 US Dist Lexis 3784 (assuming that website qualifies as "collective work," but without referencing definition of "collective work" in 17 USC §101).

Website developers are independent contractors. Therefore, under federal copyright law, a website developer, as the creator of the website, will own the copyright in it, unless the company that engages the developer has an agreement with the developer assigning the necessary rights in the website to the company. Moreover, as discussed in §4.9, the general rule under California law is that inventors own their inventions. Labor Code §2870, which permits employers to require their employees to assign certain employee inventions to the company, however, does not apply to independent contractors. For that reason, any website development agreement entered into with a third party (nonemployee) developer should contain detailed provisions on intellectual property ownership and an assignment by the developer to the company of those rights in the website that the parties have agreed the company will own. Suggested assignment provisions are set forth in Section 7.1 of the form of website development agreement in §5.25.

© The Regents of the University of California

§5.13 3. Domain Name Registration and Ownership

Domain name registration is discussed in §§3.1-3.9. In connection with website development agreements, it is important to note that businesses should register their own domain names, rather than allowing website developers to handle any part of the domain name registration process. By doing so, if the development does not work out or if the company desires to transfer website work away from the initial developer, the company will avoid the additional complication of having to resolve potential administrative or ownership issues with the domain name registrar.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/5 Website Development/§5.14 F. Drafting Website Development Agreement

§5.14 F. Drafting Website Development Agreement

A website development agreement should be in writing, and should clearly identify (1) the responsibilities of each party, (2) when items must be delivered or services performed, (3) how much development will cost and when payments are due, and (4) who will own the materials developed under the agreement. Both sides will benefit from a complete, well-written contract: Developers will know exactly what they need to do, and when, to get paid, and companies will have a clear articulation of the website to be produced under the agreement. Sections 5.15-5.22 discuss the parts of the agreement that should receive particular attention.

PRACTICE TIP: Clients should be encouraged to begin thinking about the process of drafting and negotiating their timetable for delivery of the website, including all deliveries of interim materials as well as the functional specifications that describe the website, as early in the process as possible. For any specifications and timetables that are not completed before the agreement is executed, a rigorous schedule for completion, review, and approval should be included in the agreement, so that development is not stalled by a lack of consensus over website features or the timing of development.

© The Regents of the University of California

§5.15 1. Responsibilities of Parties

Website development agreements should address the parties' respective responsibilities in detail, so that every part of the development process is allocated to one or the other of the parties. Depending on the form of agreement, a party's responsibilities may be described in the body of the agreement or may be included on an exhibit—*e.g.*, a schedule of deliverables, as described in Section 1.5 of the form of website development agreement provided in §5.25. Regardless of the chosen form of agreement, counsel must work closely with the client to ensure that contract descriptions of the parties' responsibilities, the deliverables, and the website features (as described in a functional specification or similar document) are well integrated and operate to cover all parts of the development process.

Typically, the company is responsible for providing much of the content that will be incorporated on the website, such as company logos, images, and software downloads, while the developer is responsible for developing a website (either by incorporating code that the developer owns from previous engagements or by drafting new code to meet the need) containing all of the functions identified by the company for inclusion in the website. Sometimes, a developer will utilize a substantial quantity of preexisting code to perform the agreement, and other times the developer will need to create much of the website code from scratch. The ratio of the former (sometimes called "shelf code") with the latter should be reflected in the cost of the development, and perhaps also in the allocation of ownership rights in the website. A developer with a substantial library of useful shelf code will want to retain as many rights as possible to that code, to make sure that the developer can continue using it when developing websites for other clients.

Often, at the beginning of a development project, a company does not have a clear idea of what features its website should include. The developer, however, may have a set of favorite features and templates that he or she is inclined to use in any new development project. If the website contents cannot be clearly defined before the development agreement is executed, both parties should meet and discuss the website and its features as soon as possible after execution of the agreement.

© The Regents of the University of California

§5.16 2. Deliverables and Timelines for Delivery

The agreement should include—typically as an exhibit, so that it can be amended and updated as needs change—a detailed description (often called the "functional specification") of how the website will look and how it will function. The parties should include drawings, diagrams, images—anything that will help describe the desired end product. If the agreement has a schedule of deliverables, it often includes columns identifying the deliverable, the responsible party, the due date, the process for review and approval, and the time allotted for that review and approval, although this may vary depending on how much detail the agreement includes concerning the responsibilities of the parties—with ample detail in the agreement itself, a separate schedule of deliverables may not be needed.

In many cases, payments for development of the website are tied to delivery of certain materials or completion of significant milestones by the developer. The amount of each payment may reflect the significance of the deliverable or milestone, or payments may be broken down into equal installments payable over the development timeline. The company should retain some portion of the total contract price—typically between 10 and 25 percent, but occasionally as high as fifty percent or more—until the company has reviewed and accepted the finished website.

© The Regents of the University of California

§5.17 3. Ownership and License Grants

Given the presumption of ownership in favor of an independent contractor (see §§5.11-5.12), a website development agreement must contain detailed provisions concerning ownership of the finished website and all underlying work product. When applicable, the agreement also should contain an assignment provision, assigning to the company those rights in the website and related materials that would otherwise be retained by the developer, as well as specific license grants permitting the developer to use (and, to the extent necessary, modify) any content that the company provides and any company trademarks that will be included in the website. To the extent that a developer is incorporating shelf code (see §5.15) for which the developer will retain ownership, the agreement should contain a provision granting the company a license to use that code in connection with its operation of the website.

PRACTICE TIP: Consider instances when a grant to the company alone may not be sufficiently broad—*e.g.*, when the company intends to engage a third party to host or maintain the website, or when a company has employees or subcontractors that will use the website in particular ways. If necessary, include either a right to sublicense the necessary rights, or a license grant that addresses all of the needed rights, in the website development agreement.

© The Regents of the University of California

§5.18 a. Ownership

As discussed in §5.15, it is normally in a company's interest to take complete ownership of the finished website and any underlying materials, while it is in the developer's interest to be able to reuse as much of the website code as possible in future development projects. The parties usually strike a compromise, with each party retaining ownership of any intellectual property that it brings to the table, *i.e.,* intellectual property and materials embodying intellectual property rights in existence before the effective date of the website development agreement. That allocation of ownership rights normally extends to any modifications, improvements, or enhancements to, or derivative works of, that intellectual property. In some cases, however, the modifications may effect such a transformation in the property from its pre-agreement state that detailed negotiations are required to establish each party's rights in the end product. One party may end up owning the end product while granting license rights to the other party to use those portions that it helped to develop.

Through the careful drafting of specific license rights permitting the licensee to use the intellectual property in a certain market (*e.g.*, "only for use in connection with applications in or related to the health care industry"), the parties may be able to impose restrictions or set boundaries between themselves and their respective permissible uses of the intellectual property embodied in the website. Section 5.19 discusses the importance of license rights in a website development agreement and describes some of the ways in which license rights might be used to address a company's competitive concerns when complete ownership of a website and its underlying technology may not be possible.

© The Regents of the University of California

§5.19 b. License Rights

A company that is paying a developer to develop a website often asks, "We paid for it, why don't we own it?" Counsel to the company should be prepared to explain a typical developer's reliance on shelf code (see §5.15) and to discuss with the company various ways in which license rights might be used to restrict a developer's ability to reuse materials developed under contract with the company.

Even in the rare instances when a company will own all rights in the website and its underlying technology, the developer will need limited rights to certain company materials—in particular, company content and any trade names, trademarks, and service marks to be included in the website—to permit development of the website. These rights should be narrowly tailored and limited to the term of the agreement, and the agreement should require company approval any time the developer needs to modify any company-furnished materials. Moreover, as noted in §5.17, an assignment of rights from the developer to the company should be included, so that, if any materials created or modified by the developer are not automatically deemed to be owned by the company, ownership in those materials will be transferred to the company by operation of the agreement.

In the more common situation in which ownership rights are allocated between the parties, bilateral license grants are essential. The company will need to grant the developer limited rights in any company materials included in the website, so that the developer can perform its obligations under the agreement but cannot otherwise make use of the company's materials. In addition, the developer will need to grant the company a license to use any technology and materials owned by the developer and incorporated into the website. Ideally, the term of this license grant should be perpetual, and should include any updates to those materials created by the developer after the completion of the website.

If competitive concerns exist (*e.g.*, when a website developer is likely to perform similar services for the company's competitors), the company should consider requesting an exclusive license for any developer materials that could give the company a competitive edge (*e.g.*, the developer's "shopping cart" technology for an e-commerce site). This exclusivity need not be comprehensive: A company should pay less if the developer retains the right to license its technology in noncompetitive ways, but the clause could be drafted to prohibit the developer from using its technology for the benefit of any of the company's competitors. Alternatively, the developer could be prohibited from using its technology for the benefit of any other customer for a limited period of time after completion of the website—long enough to allow the company to obtain an advantage by having a superior website.

© The Regents of the University of California

§5.20 c. Confidentiality

If a website developer will have access to any confidential information of the company, the agreement should require that the developer adhere to obligations of confidentiality and limitations on use of that information. A separate nondisclosure agreement should be considered when information is particularly sensitive or the company desires to maintain the status of certain information as a trade secret for a long period of time. For a form of nondisclosure agreement that could be modified for this purpose, see §4.11. Ultimately, a company's best protection against the unintended release of trade secret information is to limit initial disclosures of confidential information to the bare minimum required for the website developer to perform, and to ensure that all employees are educated on what company information is confidential as well as the need to prevent misuse of that information.

At the same time, companies should resist efforts by developers to impose obligations of confidentiality on any information provided by a developer. When a developer insists that it is giving the company confidential information, the developer should be required to identify that information clearly, so that the company can readily challenge any material that it does not believe to be confidential. This step will also enable the company to transfer website development services to another developer without risk that the company might be sued by the first developer for breach of a confidentiality obligation.

© The Regents of the University of California

§5.21 4. Representations and Warranties of Developer

A well-drafted website development agreement should protect the company by shifting certain risks of liability to the developer. In particular, the company should be protected from any claims of infringement arising from materials used in creating the website (other than materials provided by the company). A developer should also warrant that it owns (or is otherwise authorized to use) all content, tools, and technology used in the creation of the website, and should indemnify and hold the company harmless from any claims or liability that might result from a breach of that warranty.

A finished website, like other software products, should also come with a product warranty. This warranty may be limited to a post-completion warranty period, during which time the developer is obligated to fix problems with the website that come under the warranty at no additional charge to the company. Alternatively, the product warranty may remain in place for as long as the developer is providing services related to the website to the company.

When an agreement contains an appropriately detailed functional specification, the product warranty can be as simple as a promise by the developer that the website will at all times perform in accordance with the functional specification. If, however, the functional specification does not address matters of website performance that the company deems important, those matters should be detailed in the agreement or in an exhibit to the agreement. For example, when a company requires regular updates to the website or requires that the website appear in a prominent position on particular search engines, those requirements should be described in as much detail as possible, to avoid later disputes over whether or not the warranty has been breached. Similarly, when a company needs the developer to take certain steps to cure defects covered by the warranty, those steps should be described in as much detail as possible and should include developer response times and procedures for notifying the company when the defect has been identified and when it has been fixed.

© The Regents of the University of California

§5.22 5. Ongoing Obligations of Developer

In some cases, a developer's obligations under a website development agreement will end on delivery of the completed website, or perhaps on expiration of a warranty period that commences on delivery of the website. In many cases, however, the developer will have a number of obligations continuing beyond the date of delivery. Most important from the company's perspective should be an obligation by the developer to provide the company promptly with any updates or upgrades to developer materials that are included in the website, and to update the website as necessary to ensure that it remains compliant with any changes in web browsers or other technology on which the website relies. In addition, the developer's warranties of ownership and noninfringement, together with the related indemnification obligations, should survive any termination or expiration of the agreement. The length of the survival period will be a matter of negotiation for the parties.

Hosting, maintenance, technical support and other services that are often included as ongoing obligations of a website developer are discussed in chap 6.

© The Regents of the University of California

G. Website Development Agreements

§5.23 1. Independent Contractor Agreements

For simple website development needs—and particularly for a company that has a website but wants to improve it by adding content or features—a basic independent contractor agreement may suffice. Independent contractor agreements are discussed in §§4.13-4.21. No matter how short the agreement, it should always contain the following:

- A detailed description of the desired end product (or, if that is not possible when the parties sign the agreement, a detailed procedure for quickly arriving at such a description);
- A detailed schedule for delivery of the website product, with appropriate milestones for delivery and review along the way;
- A comprehensive allocation of intellectual property rights and a blanket assignment of rights from the developer to the company of all aspects of the website that the company intends to own; and
- A clear statement of the cost of the development services provided under the agreement and the due date(s) for payment of those costs.

Many of these provisions can be adapted from the longer form agreement included in §5.25.

© The Regents of the University of California

2. Form of Website Development Agreement

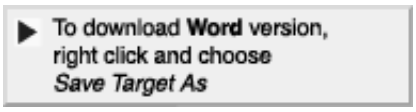
§5.24 a. Introduction

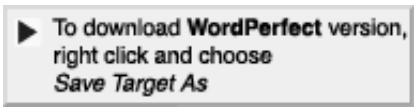
In §5.25 is a sample website development agreement that addresses the key development points discussed in §§5.11-5.23 with a slight bias in favor of the company. In using a form of agreement such as the following, it is crucial to successful completion of the development work that the parties take the time to complete all exhibits in detail, adhere to the schedule for development, and rely on the agreement's provisions to revise the schedule as needs change or unexpected hurdles arise. This form of agreement assumes that the company already owns the domain name(s) it will be using and has separately arranged for hosting of the website. For further discussion of domain name acquisition, see §§3.1-3.9; for discussion of website hosting issues, see §§6.1-6.12.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/5 Website Development/§5.25 b. Form: Website Development Agreement

§5.25 b. Form: Website Development Agreement





WEBSITE DEVELOPMENT AGREEMENT

THIS WEBSITE DEVELOPMENT AGREEMENT ("Agreement") is made as of _ _[*date*]_ _, ("Effective Date"), by and between _ _[*name of customer*]_ _ ("Customer") with offices at _ _[*address*]_ _, and _ _[*name of developer*]_ _ ("Developer") with offices at _ _[*address*]_ _, with reference to the following facts:

WHEREAS, Developer is engaged in the business of website development and other development, systems integration, maintenance, and support services; and

WHEREAS, Customer desires to retain Developer for the purpose of providing certain of the foregoing services, as further described in this Agreement;

NOW, THEREFORE, in consideration of the mutual conditions and covenants set forth herein, the receipt and sufficiency of which are hereby acknowledged, the Customer and Developer agree to the following terms and conditions:

1. DEFINITIONS. As used in this Agreement, the following terms have the following meanings:

1.1. "Content" means all data, text, pictures, sound, graphics, logos, marks, symbols, video, and other materials supplied by Customer to Developer under this Agreement, as such materials may be modified from time to time by the parties.

1.2. "Design Fee(s)" means the fee(s) set forth in Exhibit A for Development and related Services.

1.3. "Development Services" means the website development and related services described in Section 3 and Exhibit A.

1.4. "Domain Name" means the domain name specified for the Website by Customer from time to time. The initial Domain Name is specified in Exhibit A.

1.5. "Delivery Schedule" means the schedule for Development and related Services, as set forth in Exhibit A.

1.6. "Developer Tools" means any and all tools, both in object code and source code form, that Developer has already developed or that Developer independently develops or licenses from a third party, excluding any tools that Developer creates under this Agreement. By way of example, Developer Tools may include, without limitation, toolbars for maneuvering between pages, search engines, Java applets, and ActiveX controls. All Developer Tools incorporated into or used in conjunction with the Website, or used to manipulate Content for distribution on the Website, shall be set forth in Exhibit A or otherwise agreed to in writing by the parties.

1.7. "Intellectual Property Rights" means, on a worldwide basis, any and all now known or hereafter known tangible and intangible (a) rights associated with works of authorship including, without limitation, copyrights, moral rights, and mask-works, (b) trademark and trade name rights and similar rights, (c) trade secret rights, (d) patents, designs, algorithms, and other industrial property rights, (e) all other intellectual and industrial property rights of every kind and nature and however designated, whether arising by operation of law, contract, license, or otherwise, and (f) all registrations, initial applications, renewals, extensions, continuations, divisions, or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

1.8. "Services" means the Development Services.

1.9. "Specifications" means Customer's requirements set forth in Exhibit A or otherwise agreed to in writing

by the parties.

1.10. "User Content" means all data, text, pictures, sound, graphics, logos, marks, symbols, video, and other materials provided by Customer Website users.

1.11. "Website" means all software, tools, data, text, pictures, sound, graphics, logos, marks, symbols, video, and any other materials or information incorporated into, used in conjunction with, or otherwise made available on or through, pages under the Domain Name (including without limitation, Content, User Content, and Work Product).

1.12. "Work Product" means all HTML files, Java files, graphics files, animation files, data files, technology, scripts, and programs, both in object code and source code form, all documentation, and all other items and information, whether tangible or intangible and in whatever form or media, created, written, conceived, made, or discovered by Developer or any Developer Personnel in connection with the performance of this Agreement.

2. SERVICES; DEVELOPER PERSONNEL

2.1. SERVICES. Developer shall provide to Customer the Services described herein, in accordance with the terms and conditions of this Agreement and Exhibit A.

2.2. DEVELOPER TOOLS. If any Developer Tools are incorporated into or are used in conjunction with the Website, or any Developer Tools are used to manipulate Content for distribution on the Website, then Developer hereby grants to Customer a worldwide, nonexclusive, sublicensable (through multiple tiers), assignable, royalty-free, perpetual, irrevocable, fully paid-up license to use, reproduce, distribute (through multiple tiers), create derivative works of, publicly perform, publicly display, digitally perform, make, have made, sell, offer for sale, and import such Developer Tools in any media now known or hereafter known. Throughout the term of this Agreement, Developer shall provide to Customer the most current copies of any Developer Tools to which Customer has rights under this section, plus any related documentation.

2.3. DEVELOPER PERSONNEL. In no event shall Developer directly or indirectly use any subcontractors or other third parties who are not bona fide Developer employees to perform any Services under this Agreement without Customer's prior written approval. Such approved subcontractors or other third parties, if any, shall collectively constitute the "Approved Subcontractors." Developer shall use only its own employees and/or Approved Subcontractors to perform Services under this Agreement. Such employees and Approved Subcontractors shall collectively constitute the "Developer Personnel."

2.4. PERFORMANCE. Developer hereby guarantees the performance of all Developer Personnel to the full extent necessary to cause Developer to comply with Developer's obligations under this Agreement and shall ensure that all Developer Personnel shall (a) be bound by all relevant terms and conditions of this Agreement; and (b) not look to Customer for any compensation, benefits, or any other claims or liabilities of any kind related to the Services or otherwise relating to this Agreement or its implementation. Except as otherwise expressly stated in this Agreement or agreed by the parties in writing, Developer shall furnish and pay for all labor, materials, services, tools, equipment, and other resources (including without limitation, computer resources) necessary to perform the Services.

3. INITIAL WEBSITE DEVELOPMENT

3.1. DELIVERY OF CONTENT. Customer shall deliver to Developer all Content that Customer intends for Developer to incorporate into the Website (the "Content"). The Content shall be in the format(s) specified in Exhibit A.

3.2. DEVELOPMENT. For the Design Fee(s), Developer shall provide the Development and related Services specified in and according to the dates provided in Exhibit A in accordance with the Dates and Pricing and Future Interactions provisions. In no event shall the total fees for Services exceed the Fee(s) set forth in Exhibit A in the Dates and Pricing provision or except as agreed to by the parties.

3.3. PROJECT MANAGERS. Each party's primary contact for Development Services (the "Project Managers") shall be the individuals specified in Exhibit A or the person otherwise designated in writing by Customer or Developer, as the case may be.

3.4. ACCEPTANCE. Developer shall provide the Customer with a prototype of the Website for Customer's review and acceptance and a final approved version of the Website according to the dates and under the terms and conditions set forth in this Agreement and in Exhibit A. Customer shall, in its sole discretion, review and evaluate the prototype Website to assess whether it meets the applicable Specifications and meets industry and Customer standards for professional, technical, and artistic quality. If Customer rejects the prototype Website, in whole or in part, Customer may, in its sole discretion, elect either: (a) to allow the Developer to provide a corrected and revised Website for Customer's acceptance in accordance with this Section 3.4, or (b) to terminate this Agreement immediately on written notice to Developer.

4. PAYMENTS

4.1. FEES. Invoices for payments under this Agreement shall be submitted to Customer at the address specified below its signature, in arrears, after the successful completion and acceptance of each applicable milestone for Development Services. Customer shall pay properly submitted and undisputed invoices within thirty (30) days after receipt. All fees quoted include, and Developer shall pay, all sales, use, excise, and other taxes that may be levied on either party in connection with this Agreement, except for taxes based on Customer's net income.

4.2. EXPENSES. Customer shall reimburse Developer for all reasonable out-of-pocket expenses that Customer has approved in writing in advance and that Developer incurs in the performance of Services under this Agreement, including without limitation, travel and lodging expenses, long distance calls, and material and supply costs, within thirty (30) days after Customer's receipt of expense statements including appropriate receipts or other documentary evidence of the expense.

5. TERM AND TERMINATION

5.1. TERM. The term of this Agreement shall begin on the Effective Date and shall expire on Customer's final acceptance and receipt of the Customer Website and completion of all Design Services as set forth in Exhibit A, unless and until otherwise terminated in accordance with Sections 3.4(b), 5.2, 5.3, or 5.4 of this Agreement.

5.2. TERMINATION FOR CAUSE. Either party may terminate this Agreement at any time, on thirty (30) days' prior written notice to the other party, if such other party materially breaches any term or condition of this Agreement and fails to cure that breach during that thirty (30)-day period.

5.3. TERMINATION FOR CONVENIENCE. Customer may terminate this Agreement at any time and for any reason on thirty (30) days' prior written notice to Developer without liability to Developer, except as specified in Section 5.5(c). If Customer terminates this Agreement under this Section, Developer shall, at Customer's reasonable discretion, complete any work assigned or scheduled during the notice period in accordance with the terms and conditions of this Agreement.

5.4. TERMINATION FOR INSOLVENCY. Either party may terminate this Agreement at any time, on written notice to the other party, if such other party ceases to conduct business in its normal course; makes an assignment for the benefit of creditors; is liquidated or otherwise dissolved; becomes insolvent; is adjudicated bankrupt; or a receiver, trustee. or custodian is appointed for it.

5.5. CONSEQUENCES OF EXPIRATION OR TERMINATION

(a) If Developer terminates this Agreement under Section 5.2 or Section 5.4, (i) Developer shall be entitled to receive payment of all amounts then due and outstanding for Services performed under this Agreement through the effective date of termination, and (ii) neither party shall be entitled to any further payment or other compensation for such termination.

(b) If this Agreement expires under Section 5.1 or if Customer terminates this Agreement under Section 3.4(b), 5.2, 5.3, or 5.4, (i) Developer shall be entitled to receive payment of all amounts then due and outstanding for Services performed under this Agreement through the effective date of termination; (ii) Developer shall promptly deliver to Customer the then-existing Work Product (including all forms, copies, and embodiments thereof), in whatever stage of completion; (iii) Developer shall promptly provide to Customer the most current copies of any Developer Tools to which Customer has rights under Section 2.2, plus any related documentation; and (iv) neither party shall be entitled to any further payment or other compensation for such termination.

(c) In addition, without limiting the applicability of subsection (a) or (b) above, if this Agreement expires under Section 5.1, Developer shall download a copy of all software, tools, data, text, pictures, sound, graphics, logos, marks, symbols, video, and any other materials or information incorporated into, used in conjunction with, or otherwise made available on or through, the Website to a medium of Customer's choosing and deliver such materials to Customer by the close of the same business day, and shall keep the Website publicly accessible for a period of ninety (90) days following the date of such expiration or termination. If the transfer requires a change in the Domain Name, immediately on the date that the Website is no longer publicly accessible, and for a period of twelve (12) months thereafter, Developer shall maintain the Website's URL and, at such URL, provide one (1) page (including a hypertext link) that Customer may use to direct its users to its new Website or some other URL of Customer's choosing. If the transfer does not require a change in the Domain Name, Developer shall cooperate with Customer in (i) assigning a new IP address to the Domain Name as Customer may request, and (ii) transferring all operations of the Website to a new provider chosen by Customer.

5.6. SURVIVAL. Sections 2.2, 5.5, 6.1, 6.2, 8, 9, 10, 11, 12, 13.1, 13.2, 13.3, 13.11, and 13.12 shall survive any termination or expiration of this Agreement.

6. WARRANTIES AND COVENANTS

6.1. WORK PRODUCT WARRANTIES. Developer represents and warrants to Customer that no Work Product, Developer Tools, or Developer-made changes to any Content or User Content shall (a) infringe on the Intellectual Property Rights of any third party or any rights of publicity or privacy; (b) violate any law, statute, ordinance, or regulation; (c) be defamatory, trade libelous, unlawfully threatening, or unlawfully harassing; (d) be obscene, pornographic, or indecent; and (e) contain any viruses, Trojan horses, trap doors, back doors, Easter eggs, worms, time bombs, cancelbots, or other computer programming routines that are intended to damage, detrimentally interfere with, surreptitiously intercept, or expropriate any system, data, or personal information.

6.2. ADDITIONAL WARRANTIES. Developer represents and warrants to Customer that (a) the Services shall be performed in a competent and professional manner by knowledgeable, trained, and qualified personnel, using sound, professional practices; (b) the Website and all Work Product shall conform to Customer's Specifications; and (c) there is no outstanding contract, commitment, or agreement to which Developer is a party or legal impediment of any kind known to Developer that conflicts with this Agreement or that might limit, restrict, or impair the rights granted to Customer under this Agreement.

6.3. CUSTOMER COVENANTS. During the term of this Agreement, Customer shall not knowingly provide Developer with any Content that (a) infringes on the Intellectual Property Rights of any third party or any rights of publicity or privacy; (b) violates any law, statute, ordinance, or regulation; (c) is defamatory, trade libelous, unlawfully threatening, or unlawfully harassing; or (d) is obscene, pornographic, or indecent.

6.4. DISCLAIMER OF WARRANTIES. EXCEPT AS SET FORTH IN SECTIONS 6.1, 6.2, and 6.3, EACH PARTY EXPRESSLY DISCLAIMS ALL WARRANTIES OR CONDITIONS OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF TITLE, NONINFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE.

7. OWNERSHIP.

7.1. OWNERSHIP OF WORK PRODUCT. The Work Product is and shall remain the sole and exclusive property of Customer, and Customer shall retain all Intellectual Property Rights therein. If Developer is deemed to retain any Intellectual Property Rights in any Work Product under applicable law, Developer hereby irrevocably assigns to Customer all such Intellectual Property Rights. If Developer has any such Intellectual Property Rights that cannot be assigned to Customer under applicable law, Developer waives the enforcement thereof. If Developer has any such Intellectual Property Rights that cannot be assigned or waived under applicable law, Developer hereby grants to Customer an exclusive, worldwide, sublicensable (through multiple tiers), assignable, royalty-free, perpetual, irrevocable, fully paid-up license to use, reproduce, distribute (through multiple tiers), create derivative works of, publicly perform, publicly display, digitally perform, make, have made, sell, offer for sale, and import such Work Product. Developer acknowledges that there are, and may be, future rights that Customer may otherwise become entitled to with respect to the Work Product that do not yet exist, as well as new uses, media, and means and forms of exploitation throughout the world exploiting

current or future technology yet to be developed, and Developer specifically intends the foregoing assignment of rights to Customer to include all such now known or unknown uses, media, and means and forms of exploitation throughout the world.

7.2. OWNERSHIP OF CONTENT AND WEBSITE. All Content and User Content shall at all times remain the sole and exclusive property of Customer or its licensors, which shall retain all Intellectual Property Rights therein. Developer shall have no rights in such Content or User Content, other than the limited right to use it for the purposes expressly set forth in this Agreement.

8. INDEMNITY

8.1. CUSTOMER INDEMNITY. Customer shall defend Developer against any third party claim, action, suit, or proceeding alleging facts that (if true) would constitute a breach of any covenant contained in Section 6.3, and Customer shall indemnify Developer for all losses, damages, liabilities, costs, and expenses (including without limitation, reasonable attorney fees) incurred by Developer as a result of a final judgment entered against Developer in any such claim, action, suit, or proceeding.

8.2. DEVELOPER INDEMNITY. Developer shall defend Customer against any third party claim, action, suit, or proceeding (a) alleging facts that (if true) would constitute a breach of any warranty contained in Sections 6.1 or 6.2; or (b) otherwise arising from any alleged act, omission, or misrepresentation by Developer or any Developer Personnel under this Agreement. Developer shall indemnify Customer for all losses, damages, liabilities, costs, and expenses (including without limitation, reasonable attorney fees) incurred by Customer, its affiliates, or its and their officers, directors, employees, and shareholders as a result of or in connection with any such claim, action, suit, or proceeding.

8.3. INDEMNITY PROCESS. The indemnifying party's obligations under this Section 8 are conditioned on the indemnified party's (a) giving the indemnifying party prompt written notice of any claim, action, suit, or proceeding for which the indemnified party is seeking indemnity under Section 8.1 or 8.2; (b) granting control of the defense and settlement to the indemnifying party; and (c) reasonably cooperating with the indemnifying party at the indemnifying party's expense.

9. CONFIDENTIAL INFORMATION. Customer's "Confidential Information" includes all passwords used in connection with the Website (including any part of the Website made available on a password-protected server for testing and evaluation purposes), all Work Product, Content, Server Logs, and any other materials or information that Customer designates as confidential and/or proprietary, or that Developer should reasonably believe to be confidential and/or proprietary. Developer's "Confidential Information" includes the source code of any Developer Tools. Developer understands and agrees that Customer does not want any other Confidential Information of Developer, and should the parties believe that additional confidential information of Developer needs to be disclosed to Customer, the parties shall execute a separate nondisclosure agreement regarding such information. Each party shall hold the other party's Confidential Information in confidence and shall not disclose such Confidential Information to third parties nor use the other party's Confidential Information for any purpose other than the purposes of this Agreement. The foregoing restrictions on disclosure shall not apply to Confidential Information that (a) is already known by the recipient, through no wrongful act or omission of the recipient, (b) becomes publicly known, through no wrongful act or omission of the recipient, (c) is received by the recipient from a third party without a restriction on disclosure or use, or (d) is independently developed by the recipient without reference to the providing party's Confidential Information.

10. LIMITATIONS ON LIABILITY. EXCEPT WITH RESPECT TO BREACHES OF SECTIONS 7 AND 9 AND EACH PARTY'S INDEMNITY OBLIGATIONS UNDER SECTION 8, LIABILITY SHALL BE CONFINED TO ACTUAL DAMAGES AND IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR ANY LOST PROFITS OR SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY OF ANY KIND; PROVIDED, HOWEVER, THAT NOTHING CONTAINED IN THIS PARAGRAPH IS INTENDED TO LIMIT ANY OF CUSTOMER'S RIGHTS UNDER SECTION 11.11.

11. GENERAL PROVISIONS

11.1. GOVERNING LAW. This Agreement shall be governed and construed in accordance with the laws of the State of California, without reference to rules regarding conflicts of laws. Any dispute arising out of this

Agreement shall be submitted to a state or federal court sitting in _ _[c*ity, state*]_ _, which shall have the exclusive jurisdiction regarding the dispute and to which court's jurisdiction the parties irrevocably submit.

11.2. FURTHER ASSURANCES. Developer shall cooperate with Customer, both during and after the term of this Agreement, in the procurement and maintenance of Customer's rights to intellectual property created under this Agreement and to execute, when requested, any other documents deemed necessary by Customer to carry out the purpose of this Agreement.

11.3. COMPLIANCE WITH LAWS. Each party shall comply with all applicable laws and regulations in the course of performing under this Agreement.

11.4. SEVERABILITY. If any court of competent jurisdiction finds any provision of this Agreement to be invalid or unenforceable, such provision shall be interpreted to the maximum extent to which it is valid and enforceable, all as determined by such court in such action, and the remaining provisions of this Agreement shall, nevertheless, continue in full force and effect without being impaired or invalidated in any way.

11.5. HEADINGS. Headings used in this Agreement are for reference purposes only and in no way define, limit, construe, or describe the scope or extent of such section or in any way affect this Agreement.

11.6. ASSIGNMENT AND SUBCONTRACTING. This Agreement and Developer's rights, duties, and obligations hereunder are personal to Developer, and Developer may not assign its rights, delegate its duties, or subcontract its rights without the prior written consent of Customer. The parties' rights and obligations shall bind and inure to the benefit of their respective successors and permitted assigns.

11.7. INDEPENDENT CONTRACTORS. The parties to this Agreement are independent contractors, and no agency, partnership, joint venture, or employee-employer relationship is intended or created by this Agreement. Neither party shall have the power to obligate or bind the other party. Developer Personnel shall work exclusively for Developer and shall not, for any purpose, be considered employees or agents of Customer. Developer assumes full responsibility for the acts of Developer Personnel while performing Services under this Agreement and shall be solely responsible for their supervision, direction and control, compensation, benefits, and taxes.

11.8. NOTICE. Except where provided otherwise, notices under this Agreement shall be in writing and shall be deemed to have been fully given and received when delivered by hand, sent by nationally recognized overnight courier, or sent by registered or certified mail, return receipt requested, postage prepaid, and properly addressed to the offices of the respective parties at the addresses set forth below the parties' signatures.

11.9. AMENDMENT; WAIVER. This Agreement may be amended only by a written instrument signed by each of the parties. A waiver of any right under any provision of this Agreement by either party shall be valid only if such waiver is in writing and signed by the party to be charged. No waiver of any right under any provision of this Agreement on any occasion shall be a waiver of any other right or under any other provision or on any other occasion. No extension of time for performance of any obligation or act shall be deemed an extension of the time for performance of any other obligation or act.

11.10. COUNTERPARTS. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original and all of which shall be taken together and deemed to be one instrument.

11.11. INJUNCTIVE RELIEF. Developer hereby waives any right to injunctive relief or rescission and agrees that its sole and exclusive remedy for any breach or alleged breach, termination, or cancellation of this Agreement by Customer shall be an action for damages and termination of its Services hereunder. Developer acknowledges that Developer's Services are unique and that Customer may suffer irreparable harm in the event of any breach by Developer and that monetary damages in such event would be inadequate to compensate Customer. Consequently, Customer shall be entitled, notwithstanding Section 10 and in addition to monetary damages or any other available remedy, to such injunctive or other relief as may be necessary to restrain any threatened, continuing, or further breach by Developer, without showing or proving actual damage sustained by Customer and without posting a bond.

11.12. AUDIT. Developer shall maintain a complete audit trail of all financial and nonfinancial transactions resulting from this Agreement. Developer shall provide to Customer, its auditors, inspectors, regulators, and

other representatives as Customer may from time to time designate, access at all reasonable times to any facility at which Services are performed under this Agreement, to Developer Personnel, and to data and records relating to the Services for the purpose of performing audits and inspections of Customer or any Developer Personnel to (a) verify the accuracy of charges and invoices, and (b) examine the performance of Services under this Agreement. Developer shall provide to such auditors, inspectors, regulators, and representatives such assistance as they require. Developer shall cooperate fully with Customer or its designees in connection with audit functions and with regard to examinations by regulatory authorities. Customer's auditors and other representatives shall comply with Developer's reasonable security requirements. Until (a) three (3) years after any expiration or termination of this Agreement, (b) all pending matters relating to this Agreement (*e.g.,* disputes) are closed, or (c) such records, documents or other information are no longer required to meet Customer's records retention policy as such policy may be adjusted from time to time, whichever is later, Developer shall maintain and provide access on request to the records, documents, and other information required to meet Customer's audit rights under this Agreement.

11.13. ORDER OF PRECEDENCE. In the event of any conflict or inconsistency between or among the terms and conditions of this Agreement and any Exhibit, the terms and conditions of this Agreement shall control.

11.14. ENTIRE AGREEMENT. This Agreement, together with all related Exhibits and schedules, including without limitation Exhibit A attached hereto, constitutes the entire understanding and agreement between the parties with respect to the subject matter hereof and supersedes any and all prior or contemporaneous oral or written communications with respect hereto, all of which are merged in this Agreement. Neither party is relying on any warranties, representations, assurances, or inducements not expressly set forth in this Agreement.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the Effective Date.

DEVELOPER:

Date: _ _ _ _ _ _

_ _[*NAME OF DEVELOPER*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: _ _[*Signature*]_ _
Name: _ _[*Typed name*]__
Its: _ _[*Title*]_ _

_ _[*Developer's address*]_ _

CUSTOMER:

Date: _ _ _ _ _ _

_ _[*NAME OF CUSTOMER*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: _ _[*Signature*]_ _
Name: _ _[*Typed name*]__
Its: _ _[*Title*]_ _

_ _[*Customer's address*]_ _

EXHIBIT A

WORK SPECIFICATION DOCUMENT AND TERMS

This Exhibit A sets forth certain terms and conditions applicable to the Website Development Agreement to which it is attached (the "Agreement"). Capitalized terms not otherwise defined herein shall have the definitions set forth in the Agreement.

Domain Name (see Section 1.4): _____

Delivery Schedule (see Section 1.5): _____

Design Fees (see Section 1.2): _____

Dates and Pricing: _____

Future Interactions: _____

_____

Development Services: _____

Format of Content (see Section 3.1): _____

_____

Project Managers (See Section 3.3): _____

For Customer: _____

_____

For Developer: _____

_____

Specifications (see Section 1.9): [*attach additional pages as necessary*]

© The Regents of the University of California

§5.26 H. Upgrading Website

Internet technology is constantly improving, and businesses with a significant online component need to keep websites up-to-date, in terms of both company-provided content and the latest online technology. Even though website development specialists and general technology companies typically offer ongoing maintenance and website enhancement services as part of longer-term agreements, often the initial website development agreement does not outlive the website developed under it. As a result, companies doing business online should have a strategy for maintaining and upgrading their websites. Because of the legal and practical issues that an upgrade may involve, businesses should start planning this strategy as early as possible—ideally in connection with development of the initial website.

NOTE: Online retailers should be aware that their websites may need upgrades to comply with the Americans With Disabilities Act (ADA) (42 USC §§12101-12213). In *National Fed'n of the Blind v Target Corp.* (ND Cal 2006) 452 F Supp 2d 946, the plaintiffs claimed Target was in violation of the ADA, the Unruh Civil Rights Act (CC §§51-53) and the Disabled Persons Act (CC §§54-55.2) because its website was inaccessible to blind individuals. The court granted Target's motion to dismiss in part to the extent that its website offered information and services unconnected to its stores, but denied the motion in part to the extent that the plaintiffs alleged that the inaccessibility of Target's website impeded the full and equal enjoyment of goods and services offered in Target's stores. In 2007, the court certified a national class and a subclass of California residents as plaintiffs. *National Fed'n of the Blind v Target Corp.* (ND Cal 2007) 582 F Supp 2d 1185.

A website developer engaged to upgrade a website will have certain practical concerns in connection with undertaking the work. Primarily, the developer will need to understand the architecture of the existing website. Although the new developer can accomplish this with a thorough review of the existing website, a company that has planned for the upgrade process will already have copies of website architecture documents, obtained from its original website developer under the initial development agreement. If obtained as a result of careful initial planning, the documents should not be subject to confidentiality restrictions that might prevent their subsequent use by the company.

Similarly, intellectual property embodied in a company's original website must be available for use by a subsequent developer. If—as is likely the case—a company does not own all of the intellectual property in its website, the upgrade will proceed more smoothly if the company, at the time of the original website development, secured sufficient rights in the website to permit any changes that the upgrade might require. In this regard, a written website development agreement (as discussed in §§5.14-5.25) is crucial for a number of reasons. First, the written agreement will detail the company's specific rights in the website intellectual property; otherwise, the company would have only a limited, nonexclusive right to use any third party intellectual property (which includes intellectual property of the initial developer), and likely would not have any right to modify or create derivative works from that intellectual property. See *Effects Assocs., Inc. v. Cohen* (9th Cir 1990) 908 F2d 555, cert denied (1991) 498 US 1103 (in the absence of a written agreement, a nonexclusive license can be implied from conduct).

Second, the original website development agreement should include additional developer obligations that contemplate website upgrades. Company access to website source code, for example, can assist subsequent developers in understanding and upgrading an existing website. If a developer is reluctant (as many will be) to hand over source code as part of its development work, a source code escrow agreement should provide an alternative, as long as the conditions for release of the source code include a trigger for website upgrade needs. For further discussion of source code escrow agreements, see chap 15.

Finally, a company must take steps to continue to maintain ownership of any intellectual property that it contributes for use in the website, as well as ownership of any modifications to that intellectual property. Many times, company-furnished intellectual property must be modified by a developer to be suitable for inclusion in the website, and a developer may seek to assert rights in the modified content based on its contribution to it. Companies should avoid granting rights in company-furnished intellectual property to the original developer; otherwise, a subsequent developer may be reluctant to use the content as modified and will instead develop its own modifications, a costly and often

unnecessary step. By carefully drafting the initial website development agreement, a company should be able to save time and money when it seeks to upgrade the website later. If a company has concerns regarding its rights to upgrade an existing website, the upgrade process should begin with a review of the intellectual property embodied in the website and the company's agreements for use of that intellectual property.

© The Regents of the University of California

6

Hosting and Related Services

I. HOSTING AGREEMENTS
- A. Introduction §6.1
- B. Negotiating Hosting Agreement §6.2
- C. Key Hosting Agreement Terms
  - 1. Responsibilities of Host §6.3
    - a. Website Hosting §6.4
    - b. Monitoring §6.5
    - c. Access to Software §6.6
    - d. Content Uploading and Maintenance §6.7
    - e. Data Collection and Reporting §6.8
  - 2. Responsibilities of Customer §6.9
- D. Warranties §6.10
- E. Form of Hosting Services Agreement
  - 1. Introduction §6.11
  - 2. Form: Hosting Services Agreement §6.12

II. CO-LOCATION AGREEMENTS
- A. Introduction §6.13
- B. Decision to Co-Locate §6.14
- C. Co-Location Services and Customer Responsibilities
  - 1. Overview §6.15
  - 2. Customer Responsibilities §6.16
  - 3. Provider Warranties §6.17
- D. Form of Co-Location Agreement
  - 1. Introduction §6.18
  - 2. Form: Co-Location Agreement §6.19
- E. Equipment Considerations §6.20

III. SERVICE LEVEL AGREEMENTS
- A. Introduction §6.21
- B. Use of Service Level Agreements Generally
  - 1. Content §6.22
  - 2. When to Request Service Level Agreement §6.23
  - 3. Monitoring and Enforcement of Service Level Agreement Terms §6.24
- C. Standard Service Level Agreement Terms
  - 1. Availability; Uptime §6.25
  - 2. Service Levels §6.26
    - a. Low Priority Requests §6.27
    - b. Medium Priority Requests §6.28
    - c. High Priority Requests §6.29
  - 3. Response Times and Response Actions §6.30
  - 4. Service Credits and Chronic Problems §6.31
  - 5. Additional Terms §6.32
    - a. Customer Support §6.33
    - b. Performance Measurement §6.34
    - c. Reporting §6.35
- D. Service Level Agreement Forms
  - 1. Sample Short Form Service Level Agreement
    - a. Introduction §6.36
    - b. Form: Short Form Service Level Agreement §6.37
  - 2. Sample Website Hosting Service Level Agreement
    - a. Introduction §6.38
    - b. Form: Website Hosting Service Level Agreement §6.39

IV. TECHNICAL SUPPORT
- A. Introduction §6.40
- B. Obtaining Technical Support from Vendors §6.41

C. Key Issues in Obtaining Support From Vendors
1. Upgrades and New Versions §6.42
2. Support Services §6.43
3. Training and Help Desk Support §6.44
D. Technical Support and Maintenance Agreement
1. Introduction §6.45
2. Form: Technical Support and Maintenance Agreement §6.46
E. Providing Technical Support to Customers §6.47
F. Basic Technical Support Exhibit
1. Introduction §6.48
2. Form: Basic Technical Support Exhibit §6.49

© The Regents of the University of California

I. HOSTING AGREEMENTS

§6.1 A. Introduction

Sections 6.2-6.10 discuss the legal and business issues to be considered in identifying a hosting services provider (host) and negotiating with the host an agreement to provide online access, facilitate online traffic, store and secure data, and obtain server space to operate software. A company that provides website hosting services is responsible for storing and maintaining websites and other files that can be accessed online and for providing those files in response to user requests to view or interact with them. A model form of hosting agreement is in §§6.11-6.12.

The service level agreement (SLA) is an important adjunct to a hosting agreement because it addresses the technical requirements (including speed and availability) of the hosted website and other hosted content. It is discussed in detail in §§6.21-6.39. The technical support agreement, which often accompanies a hosting agreement, is discussed in §§6.40-6.49.

The following discussion focuses on the process for getting and keeping a business's website online. This process includes making sure that users are able to access the website, that the website's availability will scale in response to growth in user traffic, that the website can be updated as needed, and that any business data or other confidential information collected by or used in connection with the website is adequately protected.

© The Regents of the University of California

§6.2 B. Negotiating Hosting Agreement

Unlike website development, where a competent freelance developer might have only one or two clients, a hosting provider should be selected because of its proven ability to provide hosting services to as broad a customer base as possible. The more customers served, the more consistent and reliable a provider's services should be. As a result of their broad-based experience, hosting providers typically have developed their own forms of agreement for customers.

The large Internet service providers and web portals can offer reliable hosting services to individuals or small businesses at very attractive prices—although perhaps without some of the "frills" available from providers of customized hosting services. The large ISPs or web portals often have a standard electronic "click-wrap" agreement (see §7.3) that does not permit the customer to negotiate or change the terms. The bigger a company's hosting needs—and the more a company is willing to pay for hosting services—the more opportunity a customer will have to negotiate the terms of a hosting agreement.

Even in situations where the parties eventually prepare and sign a negotiated written hosting agreement, a business should expect the hosting provider to offer its standard form of agreement as the first draft. The extent to which a provider is willing to alter its draft will vary, as will the reasonableness of terms included in the draft. In general, however, by selecting an experienced provider with a good reputation, a business can benefit from the provider's experience with numerous prior customers. An experienced provider's form of agreement (which should reflect the kinds of terms and conditions that customers generally demand) should not be too heavily slanted in favor of the provider.

© The Regents of the University of California

C. Key Hosting Agreement Terms

§6.3 1. Responsibilities of Host

The party responsible for providing hosting services will have the key responsibilities under a hosting agreement. Chief among those responsibilities will be hosting a customer's website and other content. A range of additional services may be available, depending on a customer's needs, the nature of the relationship, and the host's size and sophistication. Sections 6.4-6.8 describe some of the host's usual responsibilities.

© The Regents of the University of California

§6.4 a. Website Hosting

The crux of any hosting arrangement is the terms of the agreement to provide hosting services for a website or websites identified by the customer. A customer may also want the host to host software or files for access by its customers or its employees. Regardless of the scope of content to be hosted, the host should undertake to provide services that will enable all authorized users to access the target materials quickly and easily. Access is typically provided in accordance with certain standards, which are often set forth in a service level agreement (see §§6.21-6.39) drafted to ensure speedy and reliable access.

© The Regents of the University of California

§6.5 b. Monitoring

A hosting agreement may require provisions for monitoring ongoing operations and use of the hosted content. Monitoring may be necessary to ensure the host's compliance with the standards set forth in the hosting agreement. Monitoring provisions should be drafted to track the standards set forth in the SLA. If there is any concern that a host may not be able to provide accurate measurements, assistance may be required from third parties that specialize in website and web traffic monitoring. Cooperating with the selected third party should be one of the host's responsibilities under the hosting agreement.

© The Regents of the University of California

§6.6 c. Access to Software

In some instances, the host will operate or provide access to software programs that customers may want to use to create, monitor, update, or enhance their websites. When access to and use of such software is part of the hosting agreement, the host's responsibilities should include provisions for license grants, maintenance and support, delivery of upgrades, and protection against infringement similar to those in a standard software license agreement. See chap 12.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/6 Hosting and Related Services/§6.7 d. Content Uploading and Maintenance

§6.7 d. Content Uploading and Maintenance

The host should be responsible for providing the tools to add, maintain, and upgrade the hosted content at a customer's direction. The hosting agreement should require a prompt response from the host any time there is a need to add or change website content. The hosting agreement may include a detailed description of the process for requesting, obtaining, and approving all changes to the hosted content.

© The Regents of the University of California

§6.8 e. Data Collection and Reporting

Depending on a company's particular needs and the nature of the hosting services it purchases, a customer may want to require that the host collect certain website usage and user data and provide that data on a regular basis in a specified format. The hosting agreement should identify the data to be collected and dictate the frequency and format of reports the host will be required to generate. Finally, unless the parties agree to a different allocation of rights in user and usage data, the agreement should make clear that the customer owns all of the data, and that the host obtains only a limited license to use the data to perform its collection and reporting obligations.

© The Regents of the University of California

§6.9 2. Responsibilities of Customer

An agreement for hosting services requires some content to be hosted. In cases where the hosting is part of a website development agreement, the host will be responsible for creating the hosted content; in most other cases, however, the host's responsibility is simply to host content that its customer provides. Accordingly, a customer should expect to provide content for the host to upload to the customer's website, and should make sure that that content remains accurate, complete, and up to date. The host will probably want customers to agree to comply with certain deadlines and turnaround times, particularly when there is a target "launch date," or when customer approval is required before changes can be posted to the website. Customers will need to confirm that any such deadlines are realistic.

PRACTICE TIP: In agreements where more than one party has responsibility to provide deliverables necessary to complete a task, such as uploading or formatting a website, it is important to avoid situations where a delay or failure by the other party or a third party causes a failure by the customer to adequately perform its assigned tasks, or, worse, risks putting the customer in breach of the agreement. To avoid these undesirable results, consider including language to the effect that:

Any delay by a party in performing its obligations hereunder (including any delay caused by a third party from whom such party is obtaining any materials to be delivered hereunder) shall cause a commensurate adjustment in any schedule agreed upon by the parties, so that the other party has the same time to perform its obligations and provide deliverables as it would have had absent such delay.

Care must be taken, however, to ensure that this does not provide a way for the host to obtain unwarranted extensions by blaming delays on third parties.

In hosting a customer's website and other copyrighted content, the host will use the copyrighted content in ways that implicate the customer's rights under the Copyright Act and possibly other intellectual property laws. See, *e.g.,* 17 USC §106 (exclusive rights in copyrighted works). As a consequence, the host will need a license from the customer to authorize reproduction, distribution, and preparation of derivative works with respect to the customer's copyrighted content. If no express license grant is included in the hosting agreement, one should be implied. The safest course for the customer, however, is an agreement that specifically grants the host only those rights needed to provide hosting services for designated customer content.

PRACTICE TIP: The hosting agreement should make clear that the customer owns and will retain all rights to its content, regardless of any additions, modifications, or other manipulations that the host may need to perform to allow the content to be hosted. The hosting agreement should also contain a reservation of rights, so that all rights not expressly granted to the host are reserved by the customer.

© The Regents of the University of California

§6.10 D. Warranties

Warranties are not always included in a hosting agreement. Particularly at the lower end of the hosting services spectrum, a host may require its customers to accept a disclaimer of all warranties, thus shifting to a customer all risk should the host fail to meet the customer's needs or expectations. In such cases, it is important for the customer to be able to terminate the hosting agreement on short notice or no notice in the event of a default by the host.

In customized hosting arrangements, the host typically commits to a certain level of service under a service level agreement (SLA) in lieu of any warranty on the hosting services or in addition to a very basic warranty. For a hosting customer, a robust and detailed SLA is often preferable to warranty protection. Remedies under an SLA can be self-executing (*i.e.,* automatically applied on the host's failure to meet the promised service levels) and often bear a direct relationship to the host's failure. For example, an hour of downtime may give the customer a certain dollar amount of hosting credit. Unless a warranty provision details specific rights and remedies available for a breach (and warranty provisions frequently do not do so), the host's breach of warranty will have little effect until it is so substantial as to merit litigation, and unless the hosting agreement is quite substantial, litigation is rarely in either party's best interest.

If the customer is in a position to negotiate a warranty, a host should agree to warrant that it will perform the hosting services up to a certain standard, such as "in a professional or workmanlike manner," or "in accordance with the highest industry standards." Similarly, a host should provide an "industry standard" warranty that its servers and any software used for hosting in connection with those servers will be free of viruses and other harmful code, and agree to take steps to prevent the introduction of viruses into the website and other hosted content. When a host is providing specialized software under license (for example, giving the customer use of a "shopping cart" or other e-commerce program), a warranty against infringement such as the one discussed in connection with software license agreements in chap 12 is often appropriate.

© The Regents of the University of California

E. Form of Hosting Services Agreement

§6.11 1. Introduction

Two factors are particularly significant in preparing a hosting services agreement: (1) the origin of the form used as a starting point and (2) the types of services required. Often, the form will originate with the hosting provider, which may resist substantial changes to the form and will likely reject any effort to substitute a different form of agreement. In such cases, the form in §6.12 should be used as a basis for comparing the provider's terms with terms that are intended to be customer-friendly or at least more neutral in their effect.

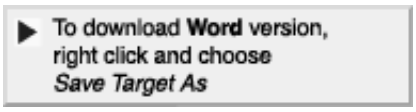
In many cases, a hosting arrangement does not stand on its own but accompanies other agreements covering some combination of website development services, technical support, or even software licenses. In such cases, the components should be integrated to the greatest extent possible into a single, comprehensive agreement, perhaps by attaching separate service agreements as exhibits to a master agreement.

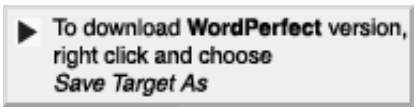
PRACTICE TIP: When a single provider is engaged to provide a range of services for a website or other online content, the areas of overlap among the different services should be considered. Any disclaimers, limitations of liability, and other provisions that typically favor a provider should be included only when relevant to a particular service. For example, while a network outage or other "force majeure" event might appropriately excuse a software or website developer's performance in creating the website or other software, such an excuse would have no place in a hosting agreement promising 100 percent uptime, when anything less than 100-percent availability, regardless of cause, should entitle a customer to service credits or other recourse against the host.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/6 Hosting and Related Services/§6.12 2. Form: Hosting Services Agreement

§6.12 2. Form: Hosting Services Agreement





HOSTING SERVICES AGREEMENT

THIS HOSTING SERVICES AGREEMENT ("Agreement") is made as of _ _[*date*]_ _ ("Effective Date"), by and between _ _[*name of customer*]_ _, a _ _[*state of incorporation*]_ _ corporation ("Customer"), and _ _[*name of provider*]_ _ ("Host").

WHEREAS, Host is engaged in the business of providing website hosting and other online delivery, maintenance, and support services.

WHEREAS, Customer desires to obtain hosting for its website(s) and other online materials, and to provide visitors to such website(s) with reliable access to the materials contained therein.

WHEREAS, Customer desires to engage Host for the purpose of providing certain of the foregoing hosting services.

NOW, THEREFORE, in consideration of the mutual conditions and covenants set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereby agree as follows:

1. DEFINITIONS. As used in this Agreement, the following terms have the following meanings:

1.1. "Customer Content" means all data, text, pictures, sound, graphics, logos, marks, symbols, video, and other materials supplied by Customer to Host pursuant to this Agreement, as such materials may be modified from time to time.

1.2. "Domain Name" means, collectively, the domain name or names specified for the Website by Customer from time to time. The initial Domain Name is _ _[*domain name*]_ _.

1.3. "Host Facility" means Host's Internet-based data center and network.

1.4. "Hosting Services" means the website hosting and other online delivery, maintenance, and support services provided by Host to Customer hereunder, as described in Section 3.1 below.

1.5. "Shadow Site" means a website that is an exact copy of the Website and is used for testing, back-up, and disaster recovery purposes.

1.6. "SLA" means the service level agreement attached hereto as Schedule 1.6.

1.7. "Term" has the meaning ascribed to it in Section 2.1, below.

1.8. "Website" means, collectively, all websites hosted by Host for Customer in the configuration and according to the terms contained in the Agreement.

2. TERM AND TERMINATION

2.1. TERM. The term of this Agreement shall commence on the Effective Date and shall continue in effect for a period of 1 year. Thereafter, this Agreement shall automatically renew for successive 1-year periods unless Customer notifies Host in writing of its desire not to renew this Agreement at least 30 days prior to the expiration of the then-current term. The initial term and any and all renewal terms are referred to herein as the "Term."

2.2. TERMINATION FOR CONVENIENCE. Customer may terminate this Agreement at any time and for any reason (including for no reason) by providing Host with at least sixty (60) days prior written notice of termination.

2.3. TERMINATION FOR BREACH. Either party may terminate this Agreement at any time on 30 days' prior written notice to the other party, if that other party materially breaches any term or condition of this Agreement and fails to cure the breach during that 30-day period.

2.4. EFFECT OF TERMINATION. Upon any expiration or early termination of this Agreement, other than a termination under Section 2.3 for a breach by Customer, Host shall, at no cost to Customer: (a) download a copy of all software, tools, data, text, pictures, sound, graphics, logos, marks, symbols, video, and any other materials or information incorporated into, used in conjunction with, or otherwise made available on or through, the Website to a medium of Customer's choosing and deliver such materials to Customer by the close of the same business day; (b) keep the Website publicly accessible for a period of ninety (90) days following the date of such expiration or termination (or such other time as the parties may agree in writing); (c) if the transfer requires a change in the Domain Name, immediately on the date that the Website is no longer publicly accessible, and for a period of 12 months thereafter, maintain the Website's URL and, at such URL, provide 1 page (including a hypertext link) that Customer may use to direct its users to its new Website or some other URL of Customer's choosing; and (d) if the transfer does not require a change in the Domain Name, cooperate with Customer in assigning a new IP address to the Domain Name as Customer may request and transferring all operations of the Website to a new provider chosen by Customer.

3. RESPONSIBILITIES OF THE PARTIES

3.1. RESPONSIBILITIES OF HOST. Commencing on the Effective Date, or such later date as the parties may agree in writing, Host shall host, maintain, and manage the Website, including access thereto, and install and maintain the equipment by which the Website is being operated, all as more fully described as follows:

(a) *Content Upload*. Host shall upload all software and other content (including without limitation the Customer Content) provided to Host for upload to the Website, as well as any updates, enhancements, and modifications thereto, within two (2) days after receipt thereof by Host.

(b) *Internet Access*. Host shall be solely responsible, at Host's expense, for acquiring, handling, maintaining, and executing any agreements for Internet access necessary to make the Website available on the Internet for access by Customer and the Website users in accordance with this Agreement and the SLA.

(c) *Website Back-Up*. Host shall make an incremental back-up of the Website every day and a complete back-up of the Website once per week. Host shall maintain off-site backup copies of the Website sufficient to ensure the continuous operation of the Website.

(d) *Host Facility*. The Host Facility (including, but not limited to, the equipment used hereunder to perform the Hosting Services) shall be secured, operated, and maintained at all times by Host in accordance with the warranties and performance standards set forth in this Agreement and in the SLA. Host shall be solely responsible, at Host's expense, for acquiring, handling, maintaining, and executing any agreements for all equipment, third party services and third party software necessary to host the Website and perform all related services hereunder. Host shall configure and operate the Host Facility so that, on receipt of a communication from a Website user, the Website can respond to such Website user in the most efficient and expeditious manner, but in no event in less than the response time set out in the SLA.

(e) *Technology Refreshing*. Host shall, at no additional cost to Customer, ensure that the Website and the Host Facility are maintained so as to be compatible with and accessible to Customer and the Website users, using the then-current developments, versions, and updates of Internet-related technology, within a reasonable time after such technology becomes generally available. In addition, to the extent that any generally available developments, versions, and updates of Internet-related technology make available any new or enhanced features or functionality that can be incorporated into the Website, Host shall provide Customer the choice to take advantage of such technical developments.

(f) *Shadow Site*. Host shall maintain the Shadow Site and operate the Shadow Site separately from the Website during the Term. Host shall make the Shadow Site available to Customer during mutually acceptable

times. All changes to the Website shall be subject to acceptance testing at the Shadow Site.

(g) *Website Capacity*. Host shall provide sufficient hosting capacity to achieve or exceed the service levels set forth in the SLA, including any capacity necessary to handle increased traffic. Customer agrees to use reasonable efforts to cooperate with Host to forecast and anticipate increases in Website traffic due to marketing events or other special circumstances that could change the rate of Website usage typically observed under normal Website operation.

(h) *Server Logs*. On the first day of every month, and at any other time as reasonably requested by Customer, Host at its expense shall deliver to Customer in electronic form (or such other form as the parties may mutually agree) the server logs of Website activity.

(i) *Return of Content*. Upon the expiration or earlier termination of this Agreement for any reason or on request by Customer at any time, but subject to Section 2.4, Host shall promptly: (a) remove and erase all copies of the Customer Content from servers within its control and use reasonable commercial efforts to remove and erase any references to Customer or the Customer Content from any site that caches, indexes, or links to the Website; and (b) return to Customer all Customer Content (and copies thereof) in tangible form.

3.2. RESPONSIBILITIES OF CUSTOMER

(a) *Content Upload*. Customer shall be entitled to upload or electronically transmit Customer Content directly to the Website. Host shall provide all support reasonably necessary to enable Customer to upload or electronically transmit Customer Content to, and/or otherwise implement modifications to Customer Content located on, the Website.

(b) *Internet Access*. Customer shall be responsible for establishing its own Internet access for Customer's interaction with the Website, and for uploading and downloading Customer Content.

(c) *License Grant*. Customer hereby grants to Host a worldwide, nonexclusive, nonsublicensable, nontransferable, royalty-free license during the Term (and for any period after termination during which Host continues to host the Website under this Agreement) to reproduce, distribute, publicly perform, publicly display, and digitally perform the Customer Content for the sole purpose of providing Hosting Services hereunder. Customer shall own and retain all right, title, and interest in and to the Customer Content (including, without limitation, any modifications thereto made by Host), and Host shall obtain no other right, title, or interest in the Customer Content except for the foregoing license.

4. RESTRICTIONS

4.1. WEBSITE. Customer shall have sole and final discretion over the form, functionality, substance, and appearance of the Website. Host shall not supplement, modify, or alter the Website, in whole or in part, without Customer's prior written consent (other than modifications strictly necessary to upload the Customer Content to the Website or otherwise necessary for the performance of Host's obligations hereunder).

4.2. HYPERTEXT LINKS. Host shall not establish or initiate any hypertext links to or from the Website, and shall not allow any third party to establish or initiate any hypertext links to and/or from the Website, without Customer's prior written consent. Host shall immediately notify Customer if Host becomes aware of any such link or attempt to link to or from the Website.

4.3. ACCESS AND SECURITY. Subject to Host's reasonable security requirements, Customer shall have access to the Host Facility in order to access any Customer equipment used for the Hosting Services.

4.4. RELOCATION OF EQUIPMENT. In the event that it becomes necessary to transfer or move the Host Facility, or to relocate the equipment used to provide Hosting Services to another physical hosting site, Host will provide Customer with the maximum possible advance written notice. Any such transfer, move, or relocation shall occur only with Customer's prior written consent, which shall not be unreasonably withheld or delayed. Host shall be solely responsible for any costs and expenses incurred in connection with any such transfer, move, or relocation and shall avoid any interruption to the Hosting Services.

5. PAYMENTS

5.1. HOSTING FEES. Invoices for payments hereunder shall be submitted to Customer at the address specified below, in arrears, after the end of each applicable calendar month for Hosting Services.

5.2. PAYMENT TERMS. Customer shall pay properly submitted and undisputed invoices within thirty (30) days after receipt. All fees quoted include, and Host shall pay, all sales, use, excise, and other taxes that may be levied on either party in connection with this Agreement, except for taxes based on Customer's net income.

6. WARRANTIES

6.1. PERFORMANCE WARRANTIES. Host represents, warrants, and covenants that: (a) the Hosting Services shall be performed in a competent and professional manner by knowledgeable, trained, and qualified personnel, using sound, professional practices; (b) Host shall use its best efforts to prevent the introduction of computer viruses into the Website and any Customer Content; and (c) there is no outstanding contract, commitment, or agreement to which Host is a party or legal impediment of any kind known to Host that conflicts with this Agreement or that might limit, restrict, or impair the ability of Host to perform this Agreement.

6.2. CUSTOMER COVENANT. During the Term of this Agreement, Customer shall not knowingly distribute on the Website any Customer Content that: (a) infringes on the intellectual property rights of any third party or any rights of publicity or privacy; (b) violates any law, statute, ordinance, or regulation; (c) is defamatory, trade libelous, unlawfully threatening, or unlawfully harassing; or (d) is obscene, pornographic, or indecent.

7. INDEMNIFICATION

7.1. CUSTOMER INDEMNITY. Customer shall defend Host against any third party claim, action, suit, or proceeding alleging facts that (if true) would constitute a breach of any covenant contained in Section 6.2, and Customer shall indemnify Host for all losses, damages, liabilities, costs, and expenses (including without limitation, reasonable attorney fees) incurred by Host as a result of a final judgment entered against Host in any such claim, action, suit, or proceeding.

7.2. HOST INDEMNITY. Host shall defend Customer against any third party claim, action, suit, or proceeding: (a) alleging facts that (if true) would constitute a breach of any warranty contained in Section 6.1; or (b) otherwise arising from any alleged act, omission, or misrepresentation by Host under this Agreement. Host shall indemnify Customer for all losses, damages, liabilities, costs, and expenses (including without limitation, reasonable attorney fees) incurred by Customer, its affiliates or its and their officers, directors, employees, and shareholders as a result of or in connection with any such claim, action, suit, or proceeding.

7.3. INDEMNITY PROCEDURE. An indemnifying party's obligations under this Section 7 are conditioned on the indemnified party: (a) giving the indemnifying party prompt written notice of any claim, action, suit, or proceeding for which the indemnified party is seeking indemnity under Section 7.1 or 7.2; (b) granting control of the defense and settlement to the indemnifying party; and (c) reasonably cooperating with the indemnifying party at the indemnifying party's expense.

8. GENERAL PROVISIONS

8.1. GOVERNING LAW. This Agreement shall be governed and construed in accordance with the laws of the State of California, without reference to rules regarding conflicts of laws. Any dispute arising out of this Agreement shall be submitted to a state or federal court sitting in _ _[*city, state*]_ _, which shall have the exclusive jurisdiction regarding the dispute and to whose jurisdiction the parties irrevocably submit.

8.2. COMPLIANCE WITH LAWS. Each party shall comply with all applicable laws and regulations in the course of performing under this Agreement.

8.3. SEVERABILITY. If any provision of this Agreement is determined by any court of competent jurisdiction to be invalid or unenforceable, such provision shall be interpreted to the maximum extent to which it is valid and enforceable, all as determined by such court in such action, and the remaining provisions of this Agreement shall, nevertheless, continue in full force and effect without being impaired or invalidated in any way.

8.4. HEADINGS. Headings used in this Agreement are for reference purposes only and in no way define,

limit, construe, or describe the scope or extent of such section or in any way affect this Agreement.

8.5. ASSIGNMENT AND SUBCONTRACTING. This Agreement and Host's rights, duties, and obligations hereunder are personal to Host, and Host may not assign its rights, delegate its duties, or subcontract its rights without the prior written consent of Customer. The parties' rights and obligations shall bind and inure to the benefit of their respective successors and permitted assigns.

8.6. INDEPENDENT CONTRACTORS. The parties to this Agreement are independent contractors, and no agency, partnership, joint venture, or employee-employer relationship is intended or created by this Agreement. Neither party shall have the power to obligate or bind the other party.

8.7. NOTICE. Except where provided otherwise, notices hereunder shall be in writing and shall be deemed to have been fully given and received when delivered by hand, sent by nationally recognized overnight courier, or sent by registered or certified mail, return receipt requested, postage prepaid, and properly addressed to the offices of the respective parties at the addresses set forth by the parties' signatures.

8.8. AMENDMENT; WAIVER. This Agreement may only be amended by a written instrument signed by each of the parties. A waiver of any right under any provision of this Agreement by either party hereunder shall be valid only if such waiver is in writing and signed by the party to be charged. No waiver of any right under any provision of this Agreement on any occasion shall be a waiver of any other right or under any other provision or on any other occasion. No extension of time for performance of any obligation or act shall be deemed an extension of the time for performance of any other obligation or act.

8.9. COUNTERPARTS. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original and all of which shall be taken together and deemed to be one instrument.

8.10. INJUNCTIVE RELIEF. Host hereby waives any right to injunctive relief or rescission and agrees that its sole and exclusive remedy for any breach or alleged breach, termination or cancellation of this Agreement by Host shall be an action for damages and termination of the Hosting Services hereunder.

8.11. ENTIRE AGREEMENT. This Agreement, together with all related exhibits and schedules, including without limitation Exhibit A attached hereto, constitutes the entire understanding and agreement between the parties with respect to the subject matter hereof and supersedes any and all prior or contemporaneous oral or written communications with respect hereto, all of which are merged herein. Neither party is relying upon any warranties, representations, assurances, or inducements not expressly set forth herein.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed in duplicate as of the date first above written.

Date: _ _ _ _ _ _

_ _[*NAME OF CUSTOMER*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _
_ _[*Customer's address*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

Date: _ _ _ _ _ _

_ _[*NAME OF HOST*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _
_ _[*Host's address*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

© The Regents of the University of California

II. CO-LOCATION AGREEMENTS

§6.13 A. Introduction

In its simplest form, co-location involves renting space at a specialized facility and installing computer server equipment—usually web servers—in that space. Sections 6.14-6.20 discuss the legal, business, and practical aspects of obtaining co-location services, including negotiating for the services and acquisition and installation of co-location hardware. Service level agreements, which should set standards for co-location services as they do for hosting services, are discussed in detail in §§6.21-6.39. Technical support, an additional service that may be available from the co-location provider, is discussed in §§6.40-6.49.

© The Regents of the University of California

§6.14 B. Decision to Co-Locate

Co-location must be distinguished from hosting. At least initially, most clients with online businesses enter into hosting arrangements (discussed in §§6.1-6.12), which shift to a host the tasks of obtaining, configuring, operating, and maintaining the hardware and most of the software required for the client's website. In contrast, businesses that choose to co-locate equipment are responsible for configuring that equipment, installing all required software, and ensuring that the equipment works as needed. A co-location provider offers customers a high-speed Internet connection, including an allocation of IP addresses, as well as a regulated power supply, climate control, and physical security. The actual preparation, installation, and ongoing operation of the equipment is mainly left to the customer.

Several factors are important to the decision to co-locate. First, a company must possess sufficient technical competence to identify, obtain, and operate the equipment to be co-located. Second, the company's technical requirements must be substantial, so that co-locating makes sense financially and offers advantages over hosting services. Finally, the co-location facility should be convenient to one of the company's offices, so that the company's equipment can be readily accessed.

© The Regents of the University of California

C. Co-Location Services and Customer Responsibilities

§6.15 1. Overview

Co-location is often viewed as a "no-frills" service marketed to companies with a high level of technical sophistication that are comfortable handling their own server configuration, installation, and maintenance. Even a company with less technical competence may find, as its online business grows, that co-location is more economical than using a hosting service. Companies should therefore become familiar with co-location options and understand when a transition to server acquisition and co-location may be advantageous.

Co-location services have several components. Of primary importance to most businesses with a substantial online presence is the Internet bandwidth that co-location provides. Bandwidth should be sufficient to handle large volumes of traffic as well as any periodic "spikes" in traffic without noticeable effects on users. Co-location providers sometimes impose substantial added charges for traffic surges. Therefore, a company that knows its traffic is likely to be marked by frequent high-volume incidents should take this into account in negotiating a payment structure for bandwidth and Internet access.

Co-location services also offer online businesses valuable storage, security, and disaster recovery advantages. By engaging a co-location provider, a company does not need to set aside and specially configure on-site space to house its servers or to provide for expansion of that space as the company grows. Co-location facilities are designed to meet these needs and are usually configured so that expansion is a simple matter. Many co-location providers offer a basic level of services (*e.g.*, fire protection, power continuity, and restrictions on access) for a base price and additional levels of service (*e.g.,* separate, locked cages or rooms for use by a single customer) at additional cost.

Finally, because co-location moves a company's server equipment off-site, the company has the benefit of round-the-clock staffing at the co-location facility and avoids potential disruption of its online operations should outages or other problems affect its own facilities. The extent to which a co-location provider's staff is available to assist its customers with equipment problems should influence a company's decision regarding the proximity of the co-location facility to the company's own offices. The more help a company can expect from co-location staff, the less critical it is that the facility be near the company's own offices.

© The Regents of the University of California

§6.16 2. Customer Responsibilities

As a co-location customer, a company should expect to perform most, if not all, of the work installing, configuring, operating, maintaining, and servicing the co-located equipment. In addition, for the protection of both the company and the co-location provider, the company will be required to restrict access to the co-location facility, *e.g.,* by maintaining for the provider's benefit a list of company personnel authorized to access the company's equipment. The company must also describe and identify with serial numbers the particular equipment to be installed at the co-location facility, for ownership and insurance purposes and to enable the co-location provider to control the movement of equipment in and out of the facility.

PRACTICE TIP: One nonstandard service a co-location customer should consider requesting from a service provider is the ability to reboot remotely, or have a server rebooted by the provider's staff, at any time of day without charge to the customer. Many co-location providers offer this service for free as part of their basic co-location services. If the service is not offered, it should be specifically requested.

Additional responsibilities of the co-location customer with respect to the equipment to be installed at the co-location facility are discussed in §6.20 below.

© The Regents of the University of California

§6.17 3. Provider Warranties

Warranties are usually not included in co-location agreements. In many cases, however, a co-location provider will commit to a certain level of service under a service level agreement (SLA) (see §§6.21-6.39) in lieu of a warranty on the services provided. As in the case of hosting services, a detailed SLA may be preferable to a warranty in the co-location agreement itself, because remedies under an SLA can be drafted to be self-executing, *i.e.,* applied automatically on any failure to meet the promised service levels. SLA remedies often bear a direct relationship to the failure in service, *e.g.,* an hour of downtime will entitle the customer to x dollars of service credit.

Customers that may be in a position to negotiate for warranties in a co-location agreement should ask the provider to guarantee a certain minimum standard for its services and facilities, such as "in a professional or workmanlike manner," or "in accordance with the highest industry standards." Providers offering extra services such as technical support or equipment maintenance should agree to warranties commensurate with the amount that the customer is paying for those services.

© The Regents of the University of California

D. Form of Co-Location Agreement

§6.18 1. Introduction

In §6.19 is a co-location provider's standard form agreement, which can be used as a starting point by customers in negotiating for co-location services. This form should assist counsel in understanding the basic terms applicable to co-location services.

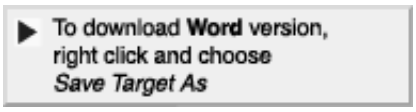
Co-location agreements should be viewed as negotiable. As the number of co-location providers grows, competition for customers increases. Clients seeking co-location services should be encouraged to interview a number of different providers and to push for revisions to a provider's form agreement. The following form reflects a bias in favor of the provider. Customers should focus on those provisions (*e.g.,* early termination fees and the disclaimer of warranties) that might be more favorably negotiated on their behalf.

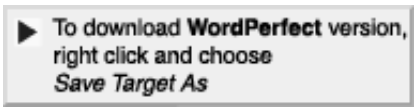
PRACTICE TIP: Because it is not uncommon for a single provider to undertake website development, equipment procurement, and hosting or co-location for an online business client, counsel should consider the areas of overlap among the different services provided and make sure that any disclaimers, limitations of liability, or other provisions favoring the provider are included only when relevant to, and appropriate for, a particular service. For example, while a network outage or other force majeure event might appropriately excuse a website developer's performance in creating the website, a force majeure clause would have no place in a co-location agreement promising 100 percent uptime, and any network outage should be a basis for a customer credit.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/6 Hosting and Related Services/§6.19 2. Form: Co-Location Agreement

§6.19 2. Form: Co-Location Agreement





CO-LOCATION AGREEMENT

THIS CO-LOCATION AGREEMENT ("Agreement") is made as of _ _[*date*]_ _ ("Effective Date"), by and between _ _[*name of customer*]_ _ ("Customer") and _ _[*name of co-location provider*]_ _ ("Provider"), with reference to the following facts:

WHEREAS, Provider is engaged in the business of providing facility space and Internet access to customers desiring to locate in Provider's facility and obtain Internet connectivity from Provider.

WHEREAS, Customer desires to locate certain servers and related equipment at Provider's facility and to connect these servers to the Internet over Provider's connection.

WHEREAS, Customer desires to engage Provider for the purpose of providing the foregoing access and facility space, as further described herein.

NOW, THEREFORE, in consideration of the mutual covenants set forth herein, and for good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. SERVICES AND CUSTOMER DATA

Exhibit 1, attached hereto and incorporated herein by this reference (the "Customer Data Sheet"), identifies the physical location ("Facility") of the equipment storage space to be made available to the Customer hereunder (the "Space"), sets forth a description of the services (the "Services") to be provided in connection with the Space and all equipment to be installed by Customer in the Space (the "Equipment"), and describes the start-up fees and monthly charges ("Start-Up Fees" and "Monthly Charges," respectively) that Customer shall pay Provider for the Space and the Services. Provider shall provide the Services to Customer at a level that meets or exceeds the service levels set forth in the service level agreement (or "SLA") attached hereto as Exhibit 3; provided, however, that the SLA also describes Customer's exclusive remedies for any failure by Provider to meet the service levels described therein.

2. TERM AND TERMINATION.

2.1. TERM. Unless otherwise specified on the Customer Data Sheet, the initial term ("Initial Term") of this Agreement shall be 1 year from the date set forth on the Customer Data Sheet (the "Term Commencement Date"). If, on completion of the Initial Term or any subsequent term (each, a "Term"), the parties do not agree to extend the Agreement for an additional Term, the Services and Space shall be provided on a month-to-month basis at the prices in effect for the prior Term.

2.2. EARLY CANCELLATION. In the event of early cancellation, Customer shall be required to pay _ _[*percent*]_ _ of the Monthly Charges for the Space for each month remaining in the Term. Customer shall remove all Equipment from the Space within 30 days after the termination of this Agreement.

3. CO-LOCATION SERVICES

3.1. USE OF SPACE

(a) Provider hereby grants Customer permission to occupy, and Customer agrees to accept, Space at the Facility subject to the terms and conditions of this Agreement. Customer may use the Space only for the purposes of installing, maintaining, and operating the Equipment. Customer may not make available space within the Space to a third party without written permission of Provider.

(b) Access to the Facility is restricted to Customer's employees and agents. Customer assumes all responsibility for all acts or omissions of the individuals authorized by Customer to enter the Facility, and agrees to indemnify and hold Provider harmless from any claims arising from the acts or omissions of these individuals. Customer's employees and agents shall comply with all applicable laws and ordinances; with the standards and practices of the telecommunications industry; and with all Provider or Facility security procedures, Facility rules, and safety practices. Provider may revoke the entry privileges of any person who fails to comply with this Agreement, who is disorderly, or who Provider reasonably suspects will violate this Agreement.

(c) Provider and its designees may observe the work activities of the Customer's employees and agents in the Facility and may inspect at any time the Equipment brought into the Space. Customer's employees and agents shall not use any products, tools, materials, or methods that, in Provider's reasonable judgment, might harm, endanger, or interfere with the Service, the Facility, or the personnel or property of Provider, its vendors, or its other customers. Provider reserves the right to take any reasonable action to prevent such potential harm.

3.2. EQUIPMENT

(a) Customer shall keep current the list of Equipment set forth on the Customer Data Sheet ("Equipment List"). Provider reserves the right to verify installation of the Equipment on the Equipment List. All Equipment must fit within the Space unless agreed to by Provider in writing. Customer agrees that all Equipment is UL approved and shall remain within the power consumption listed on Exhibit A. Cabling used by Customer must meet national electrical and fire standards. Customer shall be allowed to remove from the Facility only that Equipment listed on the then-current version of Customer's Equipment List.

(b) Customer agrees to immediately remove or render noninfringing, at Customer's expense, any Equipment alleged to infringe any patent, trademark, or copyright, or other intellectual property right.

(c) Although Provider may maintain insurance for the Facility, it does not maintain insurance for, and shall not be responsible for, any loss or damage to property of any kind owned or leased by Customer. Customer represents and covenants that it has adequate insurance coverage for the Equipment and shall maintain such insurance in effect at all times during the Term hereof. If Provider negligently or willfully damages any Equipment, Provider shall replace or repair the damaged item or, at Provider's option, shall reimburse Customer for the reasonable cost of repair or replacement.

3.3. CONDUCT

(a) Customer shall maintain and operate the Equipment in a safe manner, and keep the Space in good order and condition. No employees or agents of Customer shall harm or allow any attempt to breach security of the Facility, the Services, or any third party system or network at the Facility.

(b) Provider shall perform certain services that support the overall operation of the Facility (janitorial services, electrical, heating and cooling services, maintenance) at no additional charge to the Customer. Customer shall be required to maintain the Space in an orderly manner and shall be responsible for the prompt removal from the Facility of all trash, packing materials, boxes, or similar materials that Customer's employees or agents brought to or had delivered to the Facility.

(c) Customer's employees and agents are prohibited from bringing any of the following materials into the Facility: wet cell batteries, explosives, flammable liquids or gases, alcohol or controlled substances, weapons, cameras, or tape recorders.

(d) Customer agrees not to alter, tamper with, adjust, or repair any equipment not belonging to Customer and agrees not to erect signs or devices on the exterior of the storage cabinet or to make any construction changes or material alterations to the Space or the internal or external portions of the Facility.

4. ADDITIONAL SERVICES

All other services, including but not limited to technical assistance, network monitoring, web usage reporting, managed firewall, or other managed services are available through a third party provider, subject to

terms and conditions of a separate agreement between Customer and such third party provider.

5. PAYMENTS

5.1. FEES. Provider shall invoice the Start-Up Fees on execution and delivery of this Agreement. The Monthly Charges for Services and Space set forth on the Customer Data Sheet shall commence as of the Term Commencement Date indicated on the Customer Data Sheet. Provider shall invoice Monthly Charges monthly in arrears. Provider reserves the right to change the rates for Services and Space provided under this Agreement at any time after the Initial Term or any subsequent term by providing written notice to the customer at least 60 days in advance of the effective date of the change.

5.2. PAYMENT TERMS. Payment is due 30 days after date of invoice. Accounts are in default if payment is not received within 60 days after date of invoice. Provider reserves the right to terminate Customer's use of Space and the Services on any account unpaid after the due date and, in the event of such unpaid account, terminate any other service provided by Provider to Customer, or prohibit removal of Equipment from the Facility pending payment of all amounts owed to Provider by the Customer. The Monthly Charge for Space shall continue to accrue until Customer's Equipment is removed from the Space by Customer. An account in default is subject to an interest charge on the outstanding balance of the lesser of 1.5 percent per month or the highest rate permitted by applicable law. Customer agrees to pay Provider's reasonable expenses, including attorney and collection agency fees, incurred in enforcing its rights under this Agreement.

6. DISCLAIMERS

6.1. DISCLAIMER OF WARRANTIES. PROVIDER PROVIDES THE SPACE AND THE FACILITY ON AN "AS IS," AS AVAILABLE BASIS WITHOUT WARRANTY OF ANY KIND, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WHICH WARRANTIES PROVIDER EXPRESSLY DISCLAIMS. PROVIDER SHALL HAVE NO LIABILITY FOR FAILURE OF ANY DATA OR PRODUCT RESIDING ON CUSTOMER'S EQUIPMENT OR TRANSMITTED THROUGH THE FACILITY OR ANY PROVIDER EQUIPMENT. PROVIDER EXPRESSLY DISCLAIMS ANY REPRESENTATION OR WARRANTY THAT THE SERVICES SHALL BE ERROR-FREE OR UNINTERRUPTED.

6.2. LIMITATION OF LIABILITY. NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE SERVICE, SPACE, OR EQUIPMENT BY CUSTOMER OR ANY THIRD PARTIES. THIS INCLUDES LOST PROFITS OR LOST DATA RESULTING FROM DELAYS, NONDELIVERIES, MISDELIVERIES, SERVICE INTERRUPTIONS, POWER OR ENVIRONMENTAL CONTROL INTERRUPTION, OR DAMAGE TO THE SPACE.

6.3. NO ESTATE OR PROPERTY INTEREST. Customer acknowledges that it has been granted only a license to occupy the Space and that it has not been granted any real property interests in the Space or Facility. Payments by customer under this Agreement do not create or vest in customer (or in any other person) any leasehold estate, easement, ownership interest, or other property right or interest of any nature in any part of the facility. The parties intend that Equipment, whether or not physically affixed to the Facility, shall not be construed to be fixtures. Customer (or the lessor of the Equipment, if applicable) shall report the Equipment as its personal property whenever required by applicable laws, and shall pay all taxes levied on such Equipment.

7. INDEMNIFICATION

Customer warrants that the Space, Facility, Equipment, and Services shall not be used by Customer or any third party to conduct or engage in unlawful activities; to violate any law or regulation; to violate or infringe on the rights of any other party, including (but not limited to) contractual rights, intellectual property rights, publicity rights, or privacy rights, or in any manner that encourages conduct that would constitute a criminal offense, give rise to a civil liability, or violate any other law. Customer agrees to defend, indemnify, and hold Provider harmless from any and all claims, demands, liability, judgments, costs, and expenses (including reasonable attorney fees and costs) that arise out of or result from Customer's access to or use of the Space, Facility, Equipment, or Services, or as a result of any person claiming an ownership or possessory interest lien, trust, pledge, or security interest in any Equipment, including without limitation any attempt by such third party to take possession of the Equipment.

8. DAMAGE TO THE SPACE

8.1. If the Space is damaged by fire or other casualty, Provider shall give prompt notice to Customer of such damage, and may temporarily relocate Equipment to new space or a new facility, if practicable. If the Facility's landlord or Provider exercises an option to terminate a particular lease due to damage or destruction of the Space, or if Provider decides not to rebuild the Space, this Agreement shall terminate as of the date of the damage. Monthly Charges for the Space and Service shall proportionately abate for the period from the date of such damage.

8.2. If neither the landlord of the Facility nor Provider exercises the right to terminate, Provider shall repair the particular Space to substantially the same condition it was in prior to the damage, completing the same as soon as practical. In the event that Provider shall fail to complete the repair within a reasonable time period, Customer shall have the option to terminate this Agreement with respect to the affected Space, which option shall be the sole remedy available to Customer against Provider under this Agreement relating to such failure. If the Space or any portion thereof shall be rendered unusable by reason of such damage, the Monthly Charge for Space and Services shall proportionately abate for the period from the date of such damage to the date when such damage shall have been repaired.

9. CONFIDENTIALITY

To ensure the confidentiality of all confidential and proprietary information exchanged by them in connection with this Agreement, Customer and Provider agree to execute and deliver the mutual nondisclosure agreement attached hereto as Exhibit 2; provided, however, that if the parties have previously executed a mutual nondisclosure agreement substantially in the form of Exhibit 2, then that agreement shall instead be attached hereto as Exhibit 2 and form a part of this Agreement.

10. GENERAL PROVISIONS

10.1. GOVERNING LAW. This Agreement shall be governed and construed in accordance with the laws of the State of California, without reference to rules regarding conflicts of laws. Any dispute arising out of this Agreement shall be submitted to a state or federal court sitting in _ _[*city, state*]_ _, which shall have the exclusive jurisdiction regarding the dispute and to whose jurisdiction the parties irrevocably submit.

10.2. COMPLIANCE WITH LAWS. Each party shall comply with all applicable laws and regulations in the course of performing under this Agreement.

10.3. SEVERABILITY. If any provision of this Agreement is determined by any court of competent jurisdiction to be invalid or unenforceable, such provision shall be interpreted to the maximum extent to which it is valid and enforceable, all as determined by such court in such action, and the remaining provisions of this Agreement shall, nevertheless, continue in full force and effect without being impaired or invalidated in any way.

10.4. HEADINGS. Headings used in this Agreement are for reference purposes only and in no way define, limit, construe, or describe the scope or extent of such section or in any way affect this Agreement.

10.5. ASSIGNMENT AND SUBCONTRACTING. This Agreement and Provider's rights, duties, and obligations hereunder are personal to Provider, and Provider may not assign its rights, delegate its duties, or subcontract its rights without the prior written consent of Customer. The parties' rights and obligations shall bind and inure to the benefit of their respective successors and permitted assigns.

10.6. INDEPENDENT CONTRACTORS. The parties to this Agreement are independent contractors, and no agency, partnership, joint venture, or employee-employer relationship is intended or created by this Agreement. Neither party shall have the power to obligate or bind the other party.

10.7. NOTICE. Except where provided otherwise, notices hereunder shall be in writing and shall be deemed to have been fully given and received when delivered by hand, sent by nationally recognized overnight courier, or sent by registered or certified mail, return receipt requested, postage prepaid, and properly addressed to the offices of the respective parties at the addresses set forth by the parties' signatures.

10.8. AMENDMENT; WAIVER. This Agreement may be amended only by a written instrument signed by each of the parties. A waiver of any right under any provision of this Agreement by either party hereunder shall only be valid if such waiver is in writing and signed by the party to be charged. No waiver of any right under any

provision of this Agreement on any occasion shall be a waiver of any other right or under any other provision or on any other occasion. No extension of time for performance of any obligation or act shall be deemed an extension of the time for performance of any other obligation or act.

10.9. COUNTERPARTS. This Agreement may be executed in one or more counterparts each of which shall be deemed an original and all of which shall be taken together and deemed to be one instrument.

10.10. ENTIRE AGREEMENT. This Agreement, together with all related exhibits and schedules, including without limitation, Exhibit 1 and Exhibit 2 attached hereto, constitutes the entire understanding and agreement between the parties with respect to the subject matter hereof and supersedes any and all prior or contemporaneous oral or written communications with respect hereto, all of which are merged herein. Neither party is relying on any warranties, representations, assurances, or inducements not expressly set forth herein.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the Effective Date.

Date: _ _ _ _ _ _

_ _[*NAME OF CUSTOMER*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _
_ _[*Customer's address*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

Date: _ _ _ _ _ _

_ _[*NAME OF PROVIDER*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _
_ _[*Provider's address*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

EXHIBIT 1
CUSTOMER DATA SHEET

This "Exhibit 1: Customer Data Sheet" forms an attachment to the Co-Location Agreement executed by Customer and Provider ("Agreement") and provides certain definitions and other information relevant to such Agreement. Capitalized terms not otherwise defined in this Exhibit shall have the meanings ascribed to them in the Agreement.

"Facility" means the following equipment storage location:

_____

_____

"Services" means the following services to be provided by Provider:

_____

_____

_____

"Equipment" means the following equipment to be installed by Customer:

_____

_____

_____

_____

The "Initial Term" shall be: _____

_____

Provider's fees for the Services shall be as follows:

Start-Up Fees: _____

Monthly Charges: _____

EXHIBIT 2
NONDISCLOSURE AGREEMENT

[*Attach form of Nondisclosure Agreement*]

EXHIBIT 3
SERVICE LEVEL AGREEMENT

[*Attach form of Service Level Agreement*]

© The Regents of the University of California

§6.20 E. Equipment Considerations

Unlike customers of hosting service arrangements, in which the hosting service provider also provides the equipment used to host customer websites, co-location customers must acquire their own servers and related equipment. Equipment may be purchased or leased, under various types of financing arrangements, with differing tax and accounting consequences that are beyond the scope of this book.

A company should consider discussing its proposed equipment acquisition with its co-location provider, in case the provider has a preference for certain kinds of equipment or has learned from experience that certain equipment does not work well at the co-location facility. Companies acquiring equipment with a service contract should consider an on-site service plan, so that any necessary repairs can be done at the co-location facility. To permit on-site service, service personnel will need to be identified to the co-location provider in advance as authorized personnel. Early coordination with the service providers can help expedite repairs if equipment problems arise.

Finally, companies co-locating equipment should obtain insurance sufficient to cover the equipment located at the facility. Even if a co-location agreement does not require that the customer maintain a certain level of insurance coverage and even if the co-location provider states that it maintains insurance, the customer's own insurance policy will likely provide more complete and efficient recourse in the event of any equipment damage. In the case of natural disasters and other large-scale outages, a company's ability to deal directly with its own carrier or broker may expedite the process of obtaining replacement equipment.

© The Regents of the University of California

III. SERVICE LEVEL AGREEMENTS

§6.21 A. Introduction

A service level agreement (SLA) is an agreement that sets out the performance standards that will apply to the products and support that a service provider provides to its clients. For example, if a service provider is providing website hosting services, the SLA will specify the maximum amount of time that the website can be unavailable in any given day or month. Service level agreements are an increasingly key component of service agreements in the networked economy. Sections 6.22-6.35 focus on key issues that should be considered in drafting or negotiating service level agreements. Model forms of service level agreements are in §§6.36-6.39.

© The Regents of the University of California

B. Use of Service Level Agreements Generally

§6.22 1. Content

An SLA usually specifies standards for performance of contracted-for services, a means for identifying when performance falls below those standards, and the consequences of those performance failures (or, in some cases, incentives for meeting performance goals). Typically, a SLA is attached as an exhibit to a long-form agreement covering the core services contracted for, such as a hosting agreement or a technical support agreement. Service level agreements are indispensable in large-scale outsourcing arrangements, in which companies contract out their entire information technology departments to third party service providers, often to realize improved performance at lower costs. The SLA enables the outsourcing company to monitor the transaction to ensure that performance does not suffer and that it is obtaining the promised cost benefits.

© The Regents of the University of California

§6.23 2. When to Request Service Level Agreement

Whenever a third party inserts itself or its products into a company's network or technology infrastructure in a way that is critical to the performance of, or users' access to, that technology, it is appropriate to request an SLA from the third party. For example, a word processor installed on a single computer in an office network (or even the same word processor installed on every computer in that network) would not be an appropriate candidate for an SLA, because the word processor is not inserted into the network, but rather installed at a number of its end points. On the other hand, a word processor that is being provided by an application service provider (ASP), so that users can access and use the word processor over the network, would be an appropriate candidate for an SLA, because users' inability to access the software, or any disruptions to their use of the software, are items that should be within the control of the ASP, and for which the ASP should take responsibility.

Because so much business technology depends on networks large and small, SLAs are an appropriate way for businesses to shift the risk of network failures and downtime to their service providers. Service providers, on the other hand, may have an incentive not to offer an SLA as part of their standard agreements. They may be unwilling to subject themselves to additional obligations and possible financial loss unless they know that they are in a position to meet customary SLA standards.

© The Regents of the University of California

§6.24 3. Monitoring and Enforcement of Service Level Agreement Terms

For an SLA to be useful, it must identify the exact services to be monitored and managed by the service provider. The SLA's "teeth" are its provisions for monitoring instances of downtime or other failures to meet the agreed service levels, together with the steps that the service provider must take to remedy outages and any penalties that apply when the service provider fails to meet the service levels. Numerous third party services are available to perform necessary testing and monitoring of networks, and these services can usually be tailored to meet the needs of most technologies and budgets. When the service provider itself offers to perform monitoring, the SLA should include adequate provisions for audits of the service provider's actual performance of such monitoring and of the results that the service provider obtains when testing for network outages.

In any SLA, baseline monitoring requirements should be geared to the smallest level of network outage that must be detected. For example, if a service provider agrees to provide service credits or take other steps whenever there is an outage of more than fifteen minutes, the system should be monitored no less than once every fifteen minutes. Once the monitoring mechanisms detect an outage that triggers rights under the SLA, the SLA should specify in detail the steps that must be taken to rectify the outage.

SLAs typically describe outages and other performance failures in terms of severity or priority levels. The sample form SLA included in §6.39 contains three priority levels, ranging in severity from nonmaterial errors in the website to which the SLA applies, to complete unavailability of the website. Each priority level is associated with responses and response times, and if a problem is not handled in accordance with the SLA and resolved within the applicable response time, then the problem automatically escalates in priority level and becomes subject to a new set of requirements and response times. In this way, the SLA encourages that even minor problems be addressed in an appropriate amount of time.

A well-drafted SLA will include provisions for compensating a customer when service provider performance falls below the agreed level of uptime. In many cases, this compensation takes the form of "service credits" or similar amounts, which may be calculated, for example, on the basis of total downtime in excess of the permitted level during a measuring period (such as a month), and are available as credits against future payments due to the service provider. For many customers, the unavailability or poor performance of their website or other key network applications for even a fraction of that time could be devastating to business—and the service credit terms of an SLA should reflect that. Moreover, beyond a certain point, problems (and even minor problems that, either from lack of attention or an inability to resolve, escalate to high-priority problems) should be classified as "chronic problems," entitling the customer to demand a plan of action for resolving the problem or giving the customer a termination right. See the sample form SLA in §6.39.

© The Regents of the University of California

C. Standard Service Level Agreement Terms

§6.25 1. Availability; Uptime

The uptime guarantee may appear to be the most important term in an SLA that relates to network systems or servers, but unless the SLA includes meaningful provisions for enforcing the uptime guarantee and for crediting the customer when uptime guarantees are not met (or, viewed differently, for penalizing the service provider for failing to comply with its uptime guarantees), the uptime guarantee is merely an empty promise, without the necessary teeth to ensure that it is of value to the customer. Termination may be an overly drastic remedy when the systems or servers at issue are being held or managed by the service provider. Termination becomes a viable remedy only in more severe cases, which may leave an aggregation of smaller or persistent problems not covered by the agreement.

In the first instance, a service provider probably can be judged by the level of uptime it is prepared to guarantee. Because companies' needs and the kinds of applications available on a service-provider basis vary so widely, it is impossible to suggest any kind of standard for uptime. At the same time, there is no reason why any company should accept less than a 99-percent uptime guarantee, which works out to approximately seven hours of unavailability in a thirty-day month. Seven hours spread out over the course of 30 days may not amount to much, but what if the customer is an online retailer and all of those seven down hours occur on one day during the final shopping days before Christmas? In reviewing an SLA, always consider both the uptime percentage and the period of time over which that uptime is measured. Note, however, that exacting service levels may come with a high cost. If cost is an issue, consider inquiring about the impact of reductions in service level requirements for nonessential aspects of the services.

PRACTICE TIP: It has become customary for service providers to exclude "regularly scheduled maintenance" from their uptime guarantees. Often, the parameters of this maintenance are not explicitly disclosed in the SLA. Counsel should ask the service provider about the extent of its maintenance, as well as the times at which it is typically performed, and may also want the service provider to agree in writing that maintenance will not exceed a certain amount of time, and will only be performed during set hours (which should be selected in consultation with the client as those hours least likely to interfere with the operation of the website or other application).

© The Regents of the University of California

§6.26 2. Service Levels

The levels of service that a service provider promises to deliver will depend on the specifics of the services offered and the deal negotiated by the parties. Sections 6.27-6.29 discuss the primary levels that any SLA should include. Specific SLAs will likely include additional levels in between these three, or additional clauses specifying particular events that fall into one of these three categories. The following are examples only; actual service levels should be established based on the specific services to be rendered, the customer's needs, and the facts and circumstances involved. More service levels may provide more specificity regarding how different network or application events are handled, but they may also offer service providers the opportunity to initiate events at lower severity levels, meaning that a customer will have a longer wait for its remedy or for the event to escalate to a higher severity level.

© The Regents of the University of California

§6.27 a. Low Priority Requests

Often categorized as Priority Three (or lower), these requests for service relate to issues that disrupt the network or application only at the lowest possible level—affecting only a single user or a single, noncritical function in an application—or to issues that do not disrupt the technology at all, such as administrative requests or requests for features that do not yet exist. Typically, a service provider can quickly identify a workaround or provide an error correction for a Priority Three event. Notification of Priority Three events is often restricted to normal business hours.

© The Regents of the University of California

§6.28 b. Medium Priority Requests

Medium priority (or Priority Two) requests usually relate to problems that are not network- or application-critical, but nonetheless are disruptive to entire groups of users or affect the functionality of critical applications. Priority Two events demand prompt attention and relatively expedient resolution; in the absence of resolution, they should escalate to Priority One for treatment in accordance with the Priority One service levels. When a customer is permitted to notify the service provider of Priority Two events will depend on the specifics of each transaction, but it would certainly be appropriate in many cases for a customer to be able to provide Priority Two notification 24 hours a day, seven days a week. As an alternative, a service provider might provide a pager number for Priority Two notification, along with a requirement that any page outside of normal business hours will be answered within a short time, *e.g.,* fifteen minutes or less.

© The Regents of the University of California

§6.29 c. High Priority Requests

When an outage affects the entire application or website or the majority of a customer's users, or impacts those features critical to operation of an application, the service provider must respond promptly and with maximum resources. Priority One events can occur at any time and demand an immediate and full-scale response from the service provider. To the extent that no workaround or other short-term fix is readily identifiable, the service provider should commit personnel to the problem on a full-time basis until they find a resolution. The service provider should be in regular, if not constant, communication with its customer while remedial efforts are ongoing.

© The Regents of the University of California

§6.30 3. Response Times and Response Actions

As with service levels, response times and actions vary depending on the specifics of each transaction. Counsel should work with its client to tailor responses to fit the services being provided and the client's particular needs. Moreover, the parties can often negotiate faster response times and more detailed responses. After all, responses are only required in the event of a service outage, and no service provider should negotiate from a position of expecting to have to provide too many such responses.

To the extent that standards or rules of thumb exist, they are within the following ranges:

- **Low priority requests or events:** A request or notification must be acknowledged within several hours, and resolution of the event or completion of the event generally occurs within several days, sometimes within 24 hours.
- **Medium priority requests or events:** A request or notification must be acknowledged relatively quickly, perhaps within an hour, and resolution or completion of the event typically must occur within the day, sometimes within as few as four hours. Generally, a medium priority event not resolved within the designated time will then escalate to high-priority status.
- **High priority requests or events:** A request or notification must be acknowledged without undue delay, perhaps within minutes, and resolution of the event or completion of the event must occur as soon as possible, typically within the hour. Moreover, any failure by the service provider to remedy a high priority problem or event within the appointed time should result in service credits for the customer.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/6 Hosting and Related Services/§6.31 4. Service Credits and Chronic Problems

§6.31 4. Service Credits and Chronic Problems

A customer's remedy for a service provider's inability to meet the SLA's uptime guarantee often comes in the form of service credits or discounts, which can be used to offset future amounts that might be due to the service provider. A key feature of the SLA is the formula used to calculate the service credits, as well as the terms that specify when a customer becomes entitled to receive those credits. In addition, an SLA should include some provision for termination of the agreement to which the SLA applies if problems of network or application unavailability (or other problems that the SLA addresses) occur with a frequency that proves too disruptive to operation of the network or application. Exactly what constitutes "too disruptive" is a matter for negotiation by the parties in each transaction.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/6 Hosting and Related Services/§6.32 5. Additional Terms

§6.32 5. Additional Terms

Depending on the nature of the particular agreement to which an SLA applies, some or all of the terms discussed in §§6.33-6.35 may be appropriately included.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/6 Hosting and Related Services/§6.33 a. Customer Support

§6.33 a. Customer Support

Sometimes, an SLA contains the terms by which the service provider will provide customer and technical support to its customer. If included, these terms should specify:

- The hours of support availability;
- The kinds of support available;
- The ways in which the customer can request support; and
- The manner in which the service provider will respond to requests.

In some cases, customer support requests and responses can even be integrated into the service levels so that responses to customer support inquiries are themselves subject to service levels. Technical support is discussed in greater detail in §§6.40-6.49.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/6 Hosting and Related Services/§6.34 b. Performance Measurement

§6.34 b. Performance Measurement

Often, an SLA will specify both the performance standards to be measured and the specific tools that will be used to perform such measurement. When the accuracy of SLA measurements is of critical importance, the parties may wish to agree on a trusted third party source to conduct the measuring.

© The Regents of the University of California

§6.35 c. Reporting

In conjunction with the tools used for measurement, a service provider may be able to offer its customers reports detailing the service provider's performance of those items that are subject to the SLA. Even when a service provider does not offer such reports, a customer may want to request them. The parties can then negotiate the frequency and content of any reports that the service provider agrees to deliver.

© The Regents of the University of California

D. Service Level Agreement Forms

1. Sample Short Form Service Level Agreement

§6.36 a. Introduction

The form in §6.37 is intended for hosts and customers requiring a basic service level agreement for relatively simple hosting services, particularly in situations where a website or other hosted content is not central to the customer's business and any unavailability of the website or other hosted content will not cripple the customer's operations. Businesses that would be seriously affected by unavailability should instead consider using the longer form in §6.39. The longer form requires more detailed monitoring and reporting by the host and also requires the parties to reevaluate the designated service levels periodically and revise them, if necessary.

The short form below reflects a slight bias in favor of the customer, but is reasonable for both customer and host in several respects. For the host, the required monitoring is not especially onerous, and availability is measured over thirty-day periods. This feature tends to forgive intermittent downtime so long as availability for the whole month meets the required levels. For the customer, the higher priority service levels require a speedy response from the host, and there is good recourse (including a termination right) in the event of any chronic service problems.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/6 Hosting and Related Services/§6.37 b. Form: Short Form Service Level Agreement

§6.37 b. Form: Short Form Service Level Agreement

▶ To download **Word** version, right click and choose *Save Target As*

▶ To download **WordPerfect** version, right click and choose *Save Target As*

EXHIBIT _ _
SERVICE LEVEL AGREEMENT

This Exhibit sets forth the standards that will apply to the hosting of the Website by Host or any designee of Host authorized to provide such hosting. As used herein, "Host" refers to the party that is providing such hosting. Capitalized terms not otherwise defined in this Exhibit have the meanings ascribed to them in the _ _[*title of agreement*]_ _ ("Agreement") to which this Exhibit is attached.

1. AVAILABILITY. The Website shall have an availability of 99.5% or greater during any 30-day period during the Term of the Agreement. This availability shall include any planned or scheduled downtime (whether for server maintenance or for any other reason), as well as any and all unscheduled downtime.

2. BANDWIDTH. Bandwidth dedicated to the Website shall be as follows:

2.1. Minimum available bandwidth shall be 1.5 Mbps or greater (*i.e.,* a T1 line or greater).

2.2. When bandwidth usage reaches or exceeds 75% of the baseline available bandwidth available to the servers hosting the Website for a 5-minute peak in any 2 or more 24-hour periods in 30 days, Host shall promptly increase the minimum available bandwidth in increments of 25% or more of the baseline bandwidth until total usage remains below 75% for a 30-day period.

3. WEBSITE RESPONSE TIMES. Authorized users of the Website shall experience transmission reliability and response speeds as follows:

3.1. Roundtrip Packet Loss: Less than 5% average loss in any 30-day period.

3.2. Latency: Average response time of less than 200 milliseconds measured over 30-day periods.

4. SERVICE LEVELS AND RESPONSE ACTIONS. Service actions hereunder shall be initiated when the Host receives notification by telephone, fax, or e-mail of a network outage, or that the Website is not operating in accordance with relevant documentation. Problem reports and service requests shall be handled as follows:

[*See chart on next page*]

Service Level	**Problem**	**Availability***	**Service Actions**	
			Response Time	**Status Report**
Priority One	Complete inability to access any part of the Website, or total network unavailability. In addition, Priority Two requests that are not resolved within 24 hours after initiation	24 hours/day 7 days/week	10 minutes	20 minutes
Priority Two**	Intermittent network availability (including noncompliance with any standards set forth above) or material or critical errors	7:00 a.m.-7:00 p.m. Mon.-Thurs. 7:00 a.m.-5:00 p.m. Friday	30 minutes	60 minutes

	to portions of the Website			
Priority Three* **	Basic administrative request or identification of non-material (or other non-critical) errors in the Website	7:00 a.m.-7:00 p.m. Mon.-Thurs. 7:00 a.m.-5:00 p.m. Friday	Acknowledgement of request within 4 hours; completion of service within 3 business days after receipt of request or error report	Provided on completion of service.

*All times are Pacific Standard Time, and available days exclude U.S. holidays. For service requested outside of specified hours, requests shall be initiated on the next business day.

**Any Priority Two problem that is not corrected within 24 hours after notification shall escalate to Priority One and shall be handled in accordance with Priority One service levels.

***Any Priority Three problem that is not corrected within 3 days after Host's acknowledgement of the request shall escalate to Priority Two and shall be handled in accordance with Priority Two service levels.

5. CHRONIC PROBLEMS. If Host fails to meet the standards set forth in this Exhibit for 4 consecutive months or for any 6 months during a 12-month period, this failure shall be deemed a "Chronic Problem." Customer may give Host written notice of a Chronic Problem. Within 15 days after receipt of such notice, Host shall provide Customer with an action plan to correct the Chronic Problem. If the Chronic Problem has not been corrected within 45 days after Host receives the written notice, Customer shall be entitled to terminate the Agreement on written notice to Host.

© The Regents of the University of California

2. Sample Website Hosting Service Level Agreement

§6.38 a. Introduction

The form in §6.39 is intended for use as a hosting-specific exhibit to an agreement covering a broad range of development, hosting, and support services, or for particularly sophisticated hosting as might be provided to an e-commerce business. The form may be adapted to serve as a stand-alone hosting services agreement. Unlike the short form in §6.37, this form contemplates that the host has sophisticated monitoring capabilities. It requires the parties to negotiate the specific service levels to be applied, which are then set forth in a table of minimum service levels and response times attached to the SLA. Moreover, the applicable service levels are not treated as final upon execution. Section 2.4 of this form requires that the parties reevaluate the agreed service levels on a regular basis and make any adjustments that might be warranted by improvements in the technology or methods used to provide the hosting.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/6 Hosting and Related Services/§6.39 b. Form: Website Hosting Service Level Agreement

§6.39 b. Form: Website Hosting Service Level Agreement

▶ To download **Word** version, right click and choose *Save Target As*

▶ To download **WordPerfect** version, right click and choose *Save Target As*

EXHIBIT _ _
HOSTING SERVICE LEVELS

This Exhibit sets forth certain levels of service that Host is required to meet in performing the Hosting Services ("Hosting Service Levels"). In the case of the Hosting Service Levels designated as "Critical Service Levels," Host's failure to meet the Hosting Service Levels shall entitle Customer to receive credits against Host's fees as set forth below.

1. DEFINITIONS. Capitalized terms not otherwise defined in this Exhibit have the meanings ascribed to them in the _ _[*title of agreement*]_ _ ("Agreement") to which this Exhibit is attached. For purposes of this Exhibit, the following capitalized terms shall have the following meanings:

1.1. "Critical Service Levels" means those Hosting Service Levels designated by Customer as critical in this Exhibit.

1.2. "Downtime" means an Outage that continues for more than one minute.

1.3. "Maintenance Windows" means those time frames during which Host shall perform scheduled routine maintenance so as not to unreasonably interfere with the business needs of Customer. Host shall give Customer at least 24 hours' advance notice of routine maintenance and shall not perform routine maintenance for more than two hours at a time or outside of the hours between 2:00 a.m. and 5:00 a.m., California time, without the prior written consent of Customer.

1.4. "Outage" means any interruption of 30 seconds or more during which 2% or more of Website users are unable to access the Website or their access to the Website is substantially impaired (including through significant logon delay).

1.5. "Service Level Credit" means, with respect to a failure to meet a Critical Service Level, an amount determined by multiplying Host's Monthly Charge for the Website Hosting Services for the month in which the failure occurs by the applicable Service Level Credit Percentage for such Critical Service Level.

1.6. "Service Level Credit Percentage" means, with respect to any Critical Service Level, the maximum percentage of Host's Monthly Charge to be paid as a Service Level Credit for failure to meet the Critical Service Level.

1.7. "Service Level Default" shall be deemed to occur when Host's level of performance fails to meet a Critical Service Level.

2. SERVICE LEVEL PROCESS

2.1. SERVICE LEVEL MEASUREMENT AND REPORTING. Host shall use the necessary and appropriate measuring and monitoring tools and procedures to continuously measure the Hosting Service Levels. Host shall submit to Customer each month a performance report that documents the performance of the Hosting Services against the applicable Hosting Service Levels during the previous month. Host shall provide Customer with such information and access to such tools and procedures (including server and application monitoring tools, server logs, and network monitoring tools) as Customer may reasonably request for purposes of verifying such performance reports.

2.2. RESOLVING SERVICE LEVEL DEFAULTS. In addition to crediting Customer for any applicable Service Level Credits, if Host fails to meet any Critical Service Levels, Host shall (a) promptly investigate the causes of

the problem(s) and notify Customer of the causes of the problem(s) and the methods to be used by Host to correct the problem(s) and prevent a recurrence; (b) take those commercially reasonable actions necessary to correct the problem(s) and begin meeting the Critical Service Levels as soon as practicable; and (c) advise Customer of the status of the remedial efforts being undertaken with respect to such problem(s).

2.3. REEVALUATION OF SERVICE LEVELS AND CRITICAL SERVICE LEVELS. Sections 3 and 4 of this Exhibit identify the Hosting Service Levels and Critical Service Levels that shall apply as of the Hosting Commencement Date and during the Hosting Term, subject to the following:

(a) The numerical values associated with such Hosting Service Levels and Critical Service Levels (*e.g.,* 99.99% availability) shall be subject to Customer's and Host's mutual reevaluation 3 months after the Hosting Commencement Date. The purpose of such reevaluation shall be to confirm or change the numerical value based on the performance of Host with respect to the applicable Hosting Service Level or Critical Service Level during such 3-month period. Customer and Host may agree to adjust the Service Levels at such time.

(b) The parties agree that the Hosting Service Levels and Critical Service Levels confirmed or changed in accordance with Section 2.3(a) hereof shall not be less than those levels reasonably and consistently achievable with the systems and environments used to provide the Hosting Services if used in accordance with the practices and standards used in well-managed operations performing services similar to the Hosting Services.

2.4. IMPROVEMENTS TO SERVICE LEVELS AND CRITICAL SERVICE LEVELS. Customer and Host shall review the Service Levels at least once during the initial Hosting Term and any renewal Hosting Term and shall make adjustments to them as appropriate to reflect improved performance capabilities associated with advances in the technology and methods used to perform the Hosting Services or to reflect new information or circumstances affecting the Hosting Service Levels. During such reviews, Host shall work with Customer to identify possible cost/Hosting Service Level tradeoffs, but any resulting changes in Hosting Service Levels shall be implemented only if approved in writing by both parties. The parties expect and understand that, to the extent possible, there shall be continuous improvement in Host's delivery of the Hosting Services during the Hosting Term.

2.5. ADDITIONS/MODIFICATIONS TO HOSTING SERVICE LEVELS AND CRITICAL SERVICE LEVELS. The parties shall cooperate to identify additional Hosting Service Levels in furtherance of the objective of having a comprehensive set of Hosting Service Levels that provides a fair, accurate, and consistent measurement of Host's performance of the Hosting Services. In response to changes in Customer's business needs or to reflect changes in or evolution of the Hosting Services, Customer and Host may from time to time agree to add or substitute new Hosting Service Levels and new Critical Service Levels during the Hosting Term to meet such objective.

3. SERVICE LEVELS. Host shall meet or exceed the Hosting Service Levels described herein and in the table of minimum service levels and response times attached hereto.

3.1. WEBSITE AVAILABILITY. Host shall maintain availability of the Website to Website users so as to meet or exceed the Hosting Service Levels stated in this Exhibit. Website availability shall be calculated as follows: For a single month, the actual uptime (which shall be defined as the aggregate amount of time within the scheduled uptime that is not deemed Downtime) expressed as a percentage of the scheduled uptime less excusable downtime (*i.e.,* within the scheduled uptime, any applicable scheduled time within Maintenance Windows) for such service (i.e., Availability % = Actual Uptime/[Scheduled Uptime − Excusable Downtime] × 100). As of the Hosting Commencement Date, this Hosting Service Level shall be a Critical Service Level.

3.2. WEBSITE CAPACITY. Host shall provide sufficient hosting capacity to target the Hosting Service Levels and performance objectives in Section 3.3 of this Exhibit. Customer shall work with Host to forecast and anticipate increases in Website traffic due to unusual marketing events or other events that could change the rate of Website usage typically observed in normal Website operation. As of the Hosting Commencement Date, this Hosting Service Level shall be a Critical Service Level.

3.3. RESPONSE TIME. Host shall manage Equipment, bandwidth, and network response times to target Hosting Service Levels and performance objectives stated in this Exhibit A. As of the Hosting Commencement Date, this Hosting Service Level shall be a Critical Service Level.

4. CRITICAL SERVICE LEVELS AND SERVICE LEVEL CREDITS

4.1. EFFECT OF SERVICE LEVEL DEFAULT. Host recognizes that its failure to meet those Hosting Service Levels designated as Critical Service Levels may have a material adverse impact on the business and operations of Customer and that the damage from such failure is not susceptible to precise calculation. Accordingly, if Host fails to meet a Critical Service Level for reasons other than force majeure under the Agreement, then in addition to other remedies that may be available to Customer, Customer shall recover the corresponding Service Level Credit specified in Section 4.2 below.

4.2. SERVICE LEVEL CREDITS. In the event of a Service Level Default, the corresponding Service Level Credit shall be a credit against the Monthly Charge for Website Hosting Services owed by Customer for the month in which the Service Level Default occurs. For each such Service Level Default, the Service Level Credit shall be computed as a percentage of the total Monthly Charge for Website Hosting Services payable by Customer to Host applicable to the calendar month in which such Service Level Default occurs. If more than one Service Level Default has occurred in such calendar month, the sum of the corresponding Service Level Credits shall be credited to Customer. Each Service Level Default for Hosting Service Levels (Sections 3.1 and 3.2 hereof) and Response Time Service Levels (Section 3.3 hereof) shall result in a 40% Service Level Credit. Thus, for Downtime in any calendar month that is equal to or greater than 1% but less than 3%, the Service Level Credit shall be 40% of the Monthly Charge for Website Hosting Services. For Downtime in any calendar month that is equal to or greater than 3% but less than 5%, the Service Level Credit shall be 70% of the Monthly Charge for Website Hosting Services. For Downtime in any calendar month that is equal to or greater than 5% but less than 8%, the Service Level Credit shall be 90% of the Monthly Charge for Website Hosting Services. For Downtime in any calendar month that is equal to or greater than 8%, the Service Level Credit shall be 100% of the Monthly Charge for Website Hosting Services.

4.3. MAXIMUM SERVICE LEVEL CREDIT. The total amount of Service Level Credits actually credited to Customer with respect to Service Level Defaults occurring in a single month shall not exceed, in the aggregate, 100% of the Monthly Charge for Website Hosting Services for that month.

© The Regents of the University of California

IV. TECHNICAL SUPPORT

§6.40 A. Introduction

Technical and end-user support agreements are a two-way street for many Internet businesses and businesses with significant online or technological components. An e-business reasonably expects a certain level of support from its technology providers and other vendors; conversely, its customers expect support for the products or services marketed by it. Sections 6.41-6.44 consider both sides of this technical support equation, including the kinds of support and maintenance that vendors may be asked to provide, as well as the ways in which a business might offer its customers a certain level of support without incurring undue or unexpected costs or liabilities. A form of technical support agreement is in §6.46; a form of technical support exhibit is in §6.49.

Beyond the scope of this discussion is the role that maintenance and support agreements have begun to play in the business models of technology companies, particularly software licensors. Many software companies no longer ask customers to pay a single, up-front license fee or even an annual, software-license-only fee for use of the software. Instead, customers are asked to pay an initial license fee that entitles them to use the current version of the software and often includes maintenance and support for some initial period of time, typically a year. Thereafter, customers must pay an annual fee to continue to receive maintenance and support, and this arrangement typically represents the only way for a customer to obtain upgrades to the software when released.

Recently, the trend in pricing appeared to be headed toward increasing the up-front license fees in exchange for longer initial license and maintenance periods. This trend encountered substantial resistance, however, when customers refused to accept the higher up-front fees. See, *e.g.,* Galli, *Microsoft Tight-Lipped on Licensing Numbers*, eWeek, Aug. 2, 2002, available at http://www.eweek.com/article2/0,3959,431555,00.asp. A detailed discussion of pricing models and their relative costs and benefits is beyond the scope of this text, but possible alternative pricing models should always be considered in reviewing third party license and support plans, as well as in devising such a plan for an online business.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/6 Hosting and Related Services/§6.41 B. Obtaining Technical Support from Vendors

§6.41 B. Obtaining Technical Support from Vendors

Technical support from vendors comes in a variety of shapes and sizes. Each business must consider its own particular needs in determining whether and to what extent to enter into support agreements. This discussion will focus on software support and maintenance agreements because they are probably the most common type of support agreements for companies doing business on the Internet. Equipment maintenance and support agreements are also available, but—particularly when received directly from manufacturers—they tend to be more standardized than software support agreements, offering little room for negotiation. Nevertheless, some of the topics included in this discussion of software support agreements also apply to equipment maintenance and support agreements, and companies that undertake large equipment purchases should explore the options for support, maintenance, and repair that may be available.

PRACTICE TIP: Whenever drafting a support and maintenance agreement, whether for hardware or software, counsel should always take into account the circumstances of the specific transaction. Each transaction will differ in important details, and the following general discussion does not cover every issue that may arise.

© The Regents of the University of California

C. Key Issues in Obtaining Support From Vendors

§6.42 1. Upgrades and New Versions

A primary reason to enter into and continue a support agreement with a software vendor is to ensure access to software upgrades and new versions. Rare is the software program that is not a "work in progress," and customers should take steps to obtain the benefit of all improvements to their licensed software, however big or small. Some support agreements make a distinction between larger and smaller improvements, classifying some technical corrections (such as bug fixes, error corrections, and minor improvements) as "updates" or "upgrades" and more substantial changes (such as major rewrites, substantial functional improvements, and migrations to new operating systems) as "new versions" or "new releases."

This distinction between "updates" and "new versions" may not simply be a matter of semantics. When a support agreement draws such a distinction, the software customer should read the agreement carefully. Often the distinction is drawn so that the vendor agrees to provide only the updates for free, while reserving the right to charge additional fees to customers who want to receive the new versions. Customers should try to negotiate for inclusion of the broadest possible range of improvements—whether called upgrades, updates, new releases, new versions, or anything else—for a single maintenance fee.

Customers must also be sure that their continued receipt of support services is not conditioned on their use of upgrades that they must pay for. A vendor may try to require its customers to use only the latest release or version of its software, and may try to condition its provision of continuing support on the customers' remaining current—all of which is reasonable only if customers can stay current at no extra charge. Otherwise, the vendor is, in effect, forcing customers to pay to upgrade their software, perhaps prematurely.

© The Regents of the University of California

§6.43 2. Support Services

In addition to any charges for upgrades and new releases, the amount of a maintenance fee will depend on the kinds of support services being offered and the level of responsiveness promised by the vendor. For any software application that a business considers "mission critical" (such as credit card processing software used by a large online store), around-the-clock support service may be desirable, with the vendor agreeing to response times that are measured in minutes or hours rather than days or weeks. The manner in which support services are accessed should be as simple and inexpensive as possible. A telephone number (ideally, a toll-free telephone number) is normally preferable to an e-mail address or fax number, because the presence of a human voice on the other end of the line should offer some confirmation that a problem has been recorded and is being addressed.

At their most basic, support services provide only for reporting and handling of problems with the software. These services are often given to customers at no additional charge, because a process for recognizing and correcting problems is in the interest of both the vendor and its customers. A more detailed—and typically fee-based—support agreement will include a means by which reported problems are given priority based on severity levels, and will require the vendor to respond to certain problems within prescribed periods of time. In negotiating for rapid turnaround on severe problems, customers should identify in detail those aspects of the software that are most important to their ongoing business needs and that should therefore receive the highest priority classification (*e.g.,* "Severity Level One" or "Severity Level Two") if problems arise.

The support agreement should describe how the vendor will receive and address reported problems, including possible issuance of a tracking number to the customer in order to monitor the vendor's progress in remedying the problem. For problems of higher severity levels, some vendors will undertake to issue periodic (*e.g.,* hourly) status reports until the problem is resolved.

But problem confirmation and response should not necessarily be the sole function of support personnel. For complex, multi-function software programs, a customer may want its vendor to have dedicated staff at hand or on call to assist the customer's employees or other designated users with operation of the software. Normally, this type of service is not provided outside of business hours, and it may result in substantial additional cost to the customer. If requested, however, most vendors should be willing to provide this service.

© The Regents of the University of California

§6.44 3. Training and Help Desk Support

Occasionally, support agreements will include some discussion of training customer staff or perhaps even an agreement by the customer to establish and maintain a help desk staffed by customer personnel on the customer's premises. The help-desk personnel would be responsible for handling initial support inquiries and would follow a set of criteria designed to identify questions and problems that should be referred to the vendor for resolution. Often in this circumstance, the customer help desk is responsible for answering questions relating to use and functionality of the software, while questions relating to problems or errors are referred to the vendor. For any agreement that requires the customer to operate a help desk, the customer should negotiate with its vendor concerning the time, location, and any additional cost for training that the vendor will provide, as well as the number of customer employees that will need to be trained for the help-desk approach to succeed.

© The Regents of the University of California

D. Technical Support and Maintenance Agreement

§6.45 1. Introduction

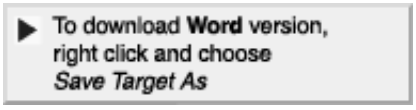
The form in §6.46 is typical of the kind of maintenance and support agreement that a provider might offer to its software licensees. It includes the concept of an annual maintenance fee, as well as suggestions for accommodating licensees who stop paying the fee but then later want to resume the support services. In addition, it provides support under two relatively broad "severity levels," and specifies the provider's maximum response times to reported problems. Two severity levels are a minimum. In some cases, a support agreement might include as many as five severity levels if the parties require a better delineation of potential software problems and want to introduce additional tiers of urgency into the provider's response obligations. Under some support agreements, if a "Severity Level One" fix is not provided almost immediately (*i.e.,* within one or two hours), the provider will owe credits to the customer. Service level agreements, discussed further in §§6.21-6.39, include similar remedies for nonperformance.

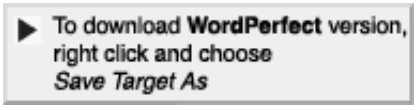
For completeness, the form in §6.46 includes a full complement of standard general provisions in Section 5. For many support agreements, particularly those intended to accompany (or even included as exhibits to) license agreements, these provisions may not be required.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/6 Hosting and Related Services/§6.46 2. Form: Technical Support and Maintenance Agreement

§6.46 2. Form: Technical Support and Maintenance Agreement





TECHNICAL SUPPORT AND MAINTENANCE AGREEMENT

THIS TECHNICAL SUPPORT AND MAINTENANCE AGREEMENT (this "Agreement") is made as of _ _[*date*]_ _ (the "Effective Date"), by and between the individual or entity identified as "Customer" below ("Customer") and _ _[*name of provider*]_ _ ("Provider"), with reference to the following facts:

WHEREAS, Customer and Provider have entered into that certain Software License Agreement dated _ _[*date*]_ _ (the "License Agreement"), which gives Customer the right to use certain software programs provided by Provider.

WHEREAS, Customer desires to obtain technical support and maintenance services for the software described above.

WHEREAS, Customer desires to engage Provider for the purpose of providing certain technical support and maintenance services, as further described herein, and Provider is willing to provide those services in accordance with the terms of this Agreement.

NOW, THEREFORE, in consideration of the mutual conditions and covenants set forth herein, and for good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. DEFINITIONS

As used in this Agreement, the following terms have the following meanings:

1.1. "Business Hours" means _ _[*time, e.g., 9 a.m.-5 p.m. (Pacific Standard Time) Monday-Friday, excluding all U.S. federal holidays*]_ _.

1.2. "Documentation" means Provider's published specifications for the software, as well as any user guides, user manuals, training materials, and other written materials or instructions that Provider provides to Customer under this Agreement or are otherwise publicly available.

1.3. "New Version" means a major release of the Software that incorporates new or additional functionality, new modules, or other substantial changes to the Software as it existed prior to such release. Provider identifies New Versions by sequential increases to the units digit of its release names (*e.g.,* V1.0, V2.0), so that releases that increase the decimal digits only (*e.g.,* V1.1, V1.25) would not constitute New Versions under this Agreement, but rather would represent Upgrades to the Software.

1.4. "Software" means the software program or programs of Provider licensed by Customer under the License Agreement.

1.5. "Term" has the meaning ascribed to it in Section 4.1 below.

1.6. "Upgrade" means any bug fix, error correction, alteration, modification, upgrade, improvement, or other change to the Software, but excluding any New Versions.

1.7. "Users" means those employees, agents, representatives, or other designees of Customer who are entitled to use the Software under the terms of the License Agreement.

2. MAINTENANCE AND SUPPORT SERVICES

2.1. GENERAL. This Agreement sets forth the terms under which Provider will provide maintenance and support to Customer for the Software licensed to Provider under the License Agreement. The use of and license to any software provided to Customer hereunder shall be governed by the terms of the License Agreement.

2.2. SUPPORT AND MAINTENANCE. Provider agrees to provide the maintenance and support specified in this Agreement, and Customer agrees to pay Provider's then-current annual support and maintenance fee, as described in Section 3.1, below. During the Term, Provider shall provide Customer and its Users with the following maintenance:

(a) *Telephone Support*. Provider shall provide telephone support to Customer and its Users by toll-free telephone number during Business Hours. On Customer's request and with Customer's prior written authorization, Provider may provide on-site support at any location specified in writing by Customer. Customer shall designate two employees, who shall be the only Customer employees entitled to request and obtain such support from Provider at any one time. On Provider's request, Customer shall provide a list with the names of the employees designated to receive support from Provider. Customer may change the names on this list at any time by providing written notice to Provider.

(b) *Error Correction*. In the event Customer or any User discovers an error in the Software that causes the Software not to operate in material conformance to the Documentation, Customer shall submit to Provider a written report describing the error in sufficient detail to permit Provider to reproduce the error. On receipt of any such written report, Provider shall classify the reported error as either: (i) a "Level 1 Severity" error, meaning an error that causes the Software to fail to operate in a material manner or to produce materially incorrect results and for which there is no workaround or only a difficult workaround; or (ii) a "Level 2 Severity" error, meaning an error that produces a situation in which the Software is usable but does not function in the most convenient or expeditious manner, and the use or value of the Software suffers no material impact. Provider shall acknowledge receipt of a conforming error report within one business day and (A) shall use its continuing best efforts to provide a correction for any Level 1 Severity error to Customer as early as practicable; and (B) shall use its reasonable efforts to include a correction for any Level 2 Severity error not later than in the next release of the Software.

[*Add one of the following alternatives*]

[*Alternative 1: Unconditional Upgrades and New Versions at Customer's request*]

(c) *Upgrades and New Versions*. Provider shall provide Customer information relating to Upgrades and New Versions of the Software during the Term. Upgrades and New Versions shall be provided to Customer by Provider at no additional charge.

[*Alternative 2: Conditional Upgrades and New Versions on Provider's terms*]

(c) *Upgrades and New Versions*. Licensee shall be entitled to receive free Upgrades during the Term, provided that Provider determines (in its sole discretion) to make Upgrades available and that Customer is current in its payment obligations hereunder. If Provider should make any New Version available during the Term, then Customer shall have the opportunity to purchase such New Version at Provider's published rates, which Provider shall make available to Customer on request.

[*Continue*]

Any New Releases or New Versions acquired by OEM shall be governed by all of the terms and provisions of the OEM Agreement.

3. PAYMENTS

3.1. MAINTENANCE FEES. In consideration of Provider's providing the maintenance and support services described herein, Customer agrees to pay Provider the initial maintenance fee set forth on Exhibit A attached hereto (the "Maintenance Fee"). This amount shall be payable for the initial term of this Agreement upon the execution hereof, and for each renewal term in advance of the commencement thereof. The Maintenance Fee may be modified by Provider for each renewal term by written notice to Customer at least 90 days prior to the end of the then-current Term. If Customer elects not to renew this Agreement for successive terms (as provided in Section 3.3 below), Customer may re-enroll only on payment of the annual Maintenance Fee for the

coming year and of all Maintenance Fees that would have been paid had Customer not ceased maintenance and support hereunder.

Comment: Payment of cumulative maintenance fees for re-enrollment is a fairly drastic requirement, and often can be negotiated down by the customer to a lesser "administrative fee."

3.2. ADDITIONAL CHARGES. In the event Provider is required to take actions to correct a difficulty or defect that is traced to Customer errors, modifications, enhancements, software, or hardware, then Customer shall compensate Provider for such actions by paying Provider its time and materials charges at its then-current hourly rates. In the event that Provider personnel must travel to perform maintenance or on-site support, and Customer has approved such travel in writing in advance, Customer shall reimburse Provider for its reasonable documented out-of-pocket expenses, including travel to and from Customer's sites, lodging, meals, and shipping, as may be necessary in connection with duties performed under Section 2 by Provider.

3.3. PAYMENT TERMS. Maintenance Fees due Provider hereunder shall be paid by Customer to the attention of the Software Licensing Department at Provider's address set forth below. Customer's initial payment shall be due on execution hereof, and payment for renewal terms shall be due on each anniversary of the Effective Date. A late payment penalty on any Maintenance Fees not paid when due shall be assessed at the rate of 1% per 30 days or the highest rate permitted by law, if lower. For additional charges incurred under Section 2 above, Customer shall pay properly submitted and undisputed invoices within 30 days after receipt. All fees quoted include, and Provider shall pay, all sales, use, excise, and other taxes that may be levied upon either party in connection with this Agreement, except for taxes based on Customer's net income.

4. TERM AND TERMINATION

4.1. TERM. The term of this Agreement shall commence on the Effective Date and shall continue in effect for a period of 1 year. Thereafter, this Agreement shall automatically renew for successive 1-year periods unless Customer notifies Provider in writing of its desire not to renew this Agreement at least 30 days prior to the expiration of the then-current term. The initial term and any and all renewal terms are referred to herein as the "Term."

4.2. TERMINATION FOR CONVENIENCE. Customer may terminate this Agreement at any time and for any reason (including for no reason) by providing Provider with at least 60 days' prior written notice of termination. In addition, this Agreement shall automatically terminate in the event that the License Agreement is terminated in accordance with its terms.

4.3. TERMINATION FOR BREACH. Either party may terminate this Agreement at any time on 30 days' prior written notice to the other party, if that other party materially breaches any term or condition of this Agreement and fails to cure the breach during that 30-day period.

4.4. EFFECT OF TERMINATION. In the event of any early termination of this Agreement by Customer, in addition to any other rights and remedies that Customer may have, Provider shall promptly refund to Customer any unused portion of the Maintenance Fee, calculated pro rata on the basis of the number of days remaining in the then-current Term. Customer understands that all of its rights under this Agreement shall cease promptly on the termination of this Agreement; provided, however, that Customer shall be entitled to continue using the then-current version of the Software, but without any Provider support, and without any Provider liability in connection with Customer's use thereof.

5. GENERAL PROVISIONS

5.1. GOVERNING LAW. This Agreement shall be governed and construed in accordance with the laws of the State of California, without reference to rules regarding of conflicts of laws. Any dispute arising out of this Agreement shall be submitted to a state or federal court sitting in _ _[*city, state*]_ _, which shall have the exclusive jurisdiction regarding the dispute and to whose jurisdiction the parties irrevocably submit.

5.2. COMPLIANCE WITH LAWS. Each party shall comply with all applicable laws and regulations in the course of performing under this Agreement.

5.3. SEVERABILITY. If any provision of this Agreement is determined by any court of competent jurisdiction to be invalid or unenforceable, such provision shall be interpreted to the maximum extent to which it is valid

and enforceable, all as determined by such court in such action, and the remaining provisions of this Agreement shall, nevertheless, continue in full force and effect without being impaired or invalidated in any way.

5.4. HEADINGS. Headings used in this Agreement are for reference purposes only and in no way define, limit, construe, or describe the scope or extent of such section or in any way affect this Agreement.

5.5. INDEPENDENT CONTRACTORS. The parties to this Agreement are independent contractors, and no agency, partnership, joint venture, or employee-employer relationship is intended or created by this Agreement. Neither party shall have the power to obligate or bind the other party.

5.6. NOTICE. Except where provided otherwise, notices hereunder shall be in writing and shall be deemed to have been fully given and received when delivered by hand, sent by nationally recognized overnight courier, or sent by registered or certified mail, return receipt requested, postage prepaid, and properly addressed to the offices of the respective parties at the addresses set forth by the parties' signatures.

5.7. AMENDMENT; WAIVER. This Agreement may only be amended by a written instrument signed by each of the parties. A waiver of any right under any provision of this Agreement by either party hereunder shall only be valid if such waiver is in writing and signed by the party to be charged. No waiver of any right under any provision of this Agreement on any occasion shall be a waiver of any other right or under any other provision or on any other occasion. No extension of time for performance of any obligation or act shall be deemed an extension of the time for performance of any other obligation or act.

5.8. COUNTERPARTS. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original and all of which shall be taken together and deemed to be one instrument.

5.9. ENTIRE AGREEMENT. This Agreement, together with all related exhibits and schedules, including without limitation Exhibit A attached hereto, constitutes the entire understanding and agreement between the parties with respect to the subject matter hereof and supersedes any and all prior or contemporaneous oral or written communications with respect hereto, all of which are merged herein. Neither party is relying upon any warranties, representations, assurances, or inducements not expressly set forth herein.

IN WITNESS WHEREOF, the undersigned have duly executed this Agreement, or have caused this Agreement to be duly executed on their behalf, as of the Effective Date.

Date: _ _ _ _ _ _

_ _[*Name of customer*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name of customer*]_ _
Its: _ _[*Title*]_ _
_ _[*Customer's address*]_ _

Date: _ _ _ _ _ _

__[*Signature*]__
_ _[*Typed name of provider*]_ _
_ _[*Provider's address*]_ _

© The Regents of the University of California

§6.47 E. Providing Technical Support to Customers

There are many ways that customers of an Internet or other technology business may request technical support. For example, a website operator might receive questions from website users on how to navigate or otherwise use the site. Depending on the amount of traffic that the website receives, these requests could quickly become overwhelming. In more complicated cases, software licensees might request training in the use of software programs, help with installing, configuring, or customizing their software, or guidance in the preparation and use of materials generated by the software. While these kinds of needs present business opportunities, they also present the risk of a substantial investment of time and resources for little to no return. For the Internet business, the important first step is to develop a company policy for handling support requests; from there, various pricing models for support services can be considered, and customers and users can be given directions on how to address their questions and support needs.

Many of the issues discussed in §§6.41-6.44 are equally applicable where a company is the provider, rather than the recipient, of technical support. Providers should identify instances where their own vendors charged (or sought to charge) for certain kinds of support services, and then consider whether they might be able to charge their customers, and thereby generate revenue, for providing similar support services.

Some companies view the need to provide technical support as an unwelcome distraction from the company's core business. Such a company could undertake to draft comprehensive documentation and help files, perhaps even a lengthy "Frequently Asked Questions" (FAQ) document, and then make clear to customers and users that no additional support will be provided outside the documentation. While substantial initial effort might be required to create the documentation, the long-term benefits could justify the effort if the documentation is effective. The documentation will need to be revised, however, as the software evolves. The company must remain attentive to the task of keeping its documentation up-to-date, and should keep in mind that this task could prove almost as much of a distraction as the support obligations that the company originally wanted to avoid.

PRACTICE TIP: Counsel should advise software providers to make a habit of updating software documentation regularly. Many times, a software license agreement's warranty will provide that the software will materially conform to "the documentation." If the documentation is drafted in detail and carefully reflects the intended features of the software, there should be little room for dispute as to whether the software does or does not so conform.

As an alternative (although more expensive than documenting the software), some companies outsource their help desk and technical support operations. In a typical situation, a call center is trained in operation of the software and in procedures for intake of error and problem reports. Once the support personnel have been trained, the company is then removed from any contact with customers, unless the company chooses to initiate it; the help desk personnel furnish reports of problems to the company for any follow-up that may be needed. For such an outsourcing arrangement to succeed, the company must ensure that the help desk personnel are sufficiently trained and that the outsourcing entity is able to warrant and meet designated service levels for response times, problem resolution, and error reporting.

© The Regents of the University of California

F. Basic Technical Support Exhibit

§6.48 1. Introduction

In many cases, the form of technical support agreement set forth in §6.46 will be more complicated than is appropriate. The following form is intended to suggest some basic support services that an Internet company might be willing to provide to its customers for no additional charge.

© The Regents of the University of California

§6.49 2. Form: Basic Technical Support Exhibit

▶ To download **Word** version, right click and choose *Save Target As*

▶ To download **WordPerfect** version, right click and choose *Save Target As*

EXHIBIT A

CUSTOMER, TECHNICAL, AND BASIC CONTENT SUPPORT SERVICES

This Customer, Technical, and Basic Content Support Services Exhibit (this "Exhibit") forms an attachment to that Master Services Agreement (the "Master Agreement") entered into by _ _[*name*]_ _ ("Provider") and _ _[*name*]_ _ ("Customer") and sets forth the technical and user support that Provider will provider to Customer and its authorized End Users pursuant to the Master Agreement. Capitalized terms not otherwise defined herein have the meanings ascribed to them in the Master Agreement.

Hours of Support Availability

7 a.m.-7 p.m. (Pacific Standard Time) Monday-Thursday

7 a.m.-5 p.m. (Pacific Standard Time) Friday

(Excluding all U.S. federal holidays)

Accessing Provider Support

Provider shall provide telephone support by toll-free number to End Users located in the United States and Canada, and End Users located in other countries may access the telephone support services during the same hours of availability through a toll number.

Provider shall further provide e-mail support and shall respond to e-mail inquiries within 24 hours of their receipt. E-mail inquiries received outside of the support hours listed above shall be deemed received at the start of the next day during which support is available. All Provider support shall be given in the English language, and Provider shall have no obligation to respond to non-English inquiries.

Customer and Technical Support

Provider customer and technical support shall address issues such as registration, login, usernames, passwords, content availability, Provider website, course navigation, browser configuration, required plug-in installation, and troubleshooting. Issues with respect to End Users' connectivity, modem, hardware configuration, Internet Service Provider, and related services are not covered by Provider's customer and technical support.

Basic Content Support

Provider shall provide standard-level content support, whereby End Users can post content-related questions on discussion boards established and operated by Provider and receive responses by e-mail in accordance with this Exhibit. Provider does not facilitate online discussions as part of its basic content support.

© The Regents of the University of California

7

Electronic Contracting

I. INTRODUCTION §7.1

II. ENFORCEABILITY OF SHRINK-WRAP, CLICK-WRAP, AND BROWSE-WRAP AGREEMENTS

A. Shrink-Wrap Software Licenses §7.2

B. Click-Wrap Agreements §7.3

C. Browse-Wrap Agreements §7.4

III. E-SIGN

A. Introduction §7.5

B. Electronic Signatures §7.6

C. Consumer Protection Features §7.7

D. Electronic Record Retention §7.8

IV. UNIFORM ELECTRONIC TRANSACTIONS ACT (UETA)

A. Overview §7.9

B. Consent Under UETA §7.10

V. UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT (UCITA) §7.11

VI. ALI SOFTWARE CONTRACT PRINCIPLES §7.12

VII. EUROPEAN UNION DIRECTIVES §7.13

VIII. CREATING ENFORCEABLE ELECTRONIC AGREEMENTS §7.14

© The Regents of the University of California

§7.1 I. INTRODUCTION

Advances in technology and mass-market distribution of computer software have challenged the traditional process of contract formation. It is not feasible to require a consumer to sign and return a software license before purchasing a word processing or other software package at a retail outlet. Similarly, any requirement that an end user physically sign and return a written agreement before entering and using an Internet website would be completely impractical to implement.

These challenges have given rise to alternative forms of contracting based on the user's acts rather than the user's signature for rights to use software and Internet-based functions. For example:

- A "shrink-wrap" license agreement refers to a contract formed when a user opens the software's packaging (often plastic shrink-wrap) and begins using the software.
- A "click-wrap" agreement is a contract formed by a user's action of clicking on a button or icon on a web page or screen launched as part of the installation of the program on the user's computer to indicate acceptance of contract terms.
- A "browse-wrap" or "click-free" agreement is a contract formed by a user's action of simply visiting or viewing an Internet website.

NOTE: Shrink-wrap and click-wrap software license agreements are commonly (and more properly) referred to as end-user license agreements, or EULAs.

Click-wrap and browse-wrap formats are used for many types of agreements and consents relating to the Internet, including

- Software license agreements (see chap 12);
- Linking agreements (see §8.18);
- Website terms of use (see §8.3); and
- Privacy policies (see §§9.44, 9.46).

Sections 7.2-7.13 provide an overview of the issues concerning the enforceability of agreements in these formats, as well as recent legislation governing enforcement of electronic contracts generally, including the federal Electronic Signatures in Global and National Commerce Act (E-Sign) (15 USC §§7001-7031) (see §§7.5-7.8); the state-level Uniform Electronic Transactions Act (UETA) (see CC §§1633.1-1633.17) (see §§7.9-7.10); the apparently ill-fated Uniform Computer Information Transactions Act (UCITA) (see §7.11); and applicable European Union directives (see §7.12). Section 7.13 includes tips for drafting enforceable online agreements.

For a detailed checklist of suggestions for maximizing the enforceability of online contracts, see Ballon, E-Commerce & Internet Law: Treatise with Forms §21.05 (2d ed 2009).

© The Regents of the University of California

II. ENFORCEABILITY OF SHRINK-WRAP, CLICK-WRAP, AND BROWSE-WRAP AGREEMENTS

§7.2 A. Shrink-Wrap Software Licenses

Courts originally viewed the enforceability of so-called "shrink-wrap" mass market software license agreements with skepticism, holding that contract terms hidden "inside the box" would not be enforceable because any contract was formed at the time of purchase and delivery of the box, not later when the box was opened. See, *e.g., Step-Saver Data Sys. v Wyse Technol.* (3d Cir 1991) 939 F2d 91 (shrink-wrap license that purchaser saw for first time on opening software was ineffective under UCC §2-207 to subsequently modify the terms of contract formed on acceptance of offer); *Vault Corp. v Quaid Software Ltd.* (5th Cir 1988) 847 F2d 255 (shrink-wrap license at issue was "contract of adhesion").

The modern view is reflected in *ProCD, Inc. v Zeidenberg* (7th Cir 1996) 86 F3d 1447, which continues to be the leading case on enforceability of shrink-wrap licenses. In *ProCD*, the Seventh Circuit held that a shrink-wrap license will be enforceable if (1) customers have an opportunity to review the terms of the license before making a final decision regarding use of the software, and (2) the license contains no contract terms that are unconscionable. In so holding, the Seventh Circuit relied on UCC §2-204(1), which provides that "[a] contract for sale of goods may be made in any manner sufficient to show agreement, including conduct by both parties which recognizes the existence of such a contract," and UCC §2-606(1)(b), which provides that a buyer is deemed to have accepted goods when, after an opportunity to inspect, he or she fails to make an effective rejection. 86 F3d at 1452. The court found that a customer may signal agreement to the terms of the license by installing and using the software, regardless of whether he or she actually took the time to read the license. Only an opportunity to review is needed. Importantly, the Seventh Circuit also held that the issue of enforceability of the license was a matter of state law, not preempted by the Copyright Act. See also *Hill v Gateway 2000, Inc.* (7th Cir 1997) 105 F3d 1147 (plaintiffs accepted terms of unread license agreement shipped with computer by using computer).

© The Regents of the University of California

§7.3 B. Click-Wrap Agreements

Specific terms of online click-wrap agreements between users and software or service providers have been upheld in many cases. *CompuServe, Inc. v Patterson* (6th Cir 1996) 89 F3d 1257 was one of the first cases holding that a contract could be formed when a user indicates acceptance by interacting with a website. In that case, the Sixth Circuit upheld a forum selection clause in an online click-wrap agreement, which required the user to type "AGREE" at several points in the online document to indicate consent to its terms. The forum selection clause at issue was in a separate agreement incorporated by reference into the main registration agreement. The court found that the user's online conduct manifested assent to the terms of the main agreement as well as to the agreement incorporated by reference. See also *MySpace, Inc. v The Globe.com, Inc.* (CD Cal, Feb. 27, 2007, No. CV 06-3391-RGK (JCx)) 2007 WL 1686966 (MySpace click-through terms of service agreement enforced); *Koresko v RealNetworks, Inc*. (ED Cal 2003) 291 F Supp 2d 1157 (plaintiff clicked box on web page marked "I agree"; agreement enforced); *Caspi v Microsoft Network, LLC* (NJ Super 1999) 732 A2d 528 (upholding forum selection clause in Microsoft Network's click-wrap membership agreement; subscribers were prompted to click either "I Agree" or "I Don't Agree" icons after scrolling through online agreement). In *Forrest v Verizon Communications, Inc*. (DC App 2002) 805 A2d 1007, the court enforced an online agreement entered into by clicking an "Accept" button below the window containing the text of the agreement. The web page cautioned users to read the agreement carefully. The court noted, "A contract is no less a contract simply because it is entered into via a computer." 805 A2d at 1011.

In *American Eyewear v Peeper's Sunglasses* (ND Tex 2000) 106 F Supp 2d 895, the court recommended the use of click-wrap agreements to avoid venue disputes, recognizing that operating a business on the Internet may potentially subject the website owner to the laws of multiple jurisdictions. For further discussion of jurisdictional issues in doing business online, see chap 19.

The federal district court in *Hotmail Corp. v Van$ Money Pie, Inc.* (ND Cal, Apr. 16, 1998, C98-20064-JW) 1998 US Dist Lexis 10729 enforced a click-wrap agreement that prohibited users of Hotmail's e-mail service from distributing spam through their Hotmail accounts. The court found that the defendant had agreed to the restriction by clicking an acceptance button indicating consent to Hotmail's online click-wrap agreement.

A Virginia court held that a click-wrap agreement was enforceable against minors despite a state statute, similar to Fam C §§6700-6710, providing that contracts by minors are voidable on the part of the minor. The court based its decision on the benefits that the students received from the Internet site, which furnished a service on behalf of schools for the submission of student papers online. *A.V. v iParadigms* (ED Va 2008) 544 F Supp 2d 473, aff'd in part and rev'd in part on other grounds (4th Cir 2009) 562 F3d 630.

NOTE: The National Conference of Commissioners on Uniform State Laws amended UCC Article 2 in 2003, including UCC §2-204(1), which now provides that a contract for sale of goods may be made "in any manner sufficient to show agreement," including "the interaction of electronic agents, and the interaction of an electronic agent and an individual." California has not yet adopted the revised Article 2, however.

© The Regents of the University of California

§7.4 C. Browse-Wrap Agreements

Browse-wrap (or click-free) agreements are documents—such as terms of use, privacy policy statements, or software license modifications—posted on a website that do not require users to affirmatively interact with the site to show their consent to the document terms. Unlike a click-wrap agreement, a browse-wrap agreement "does not require the user to manifest assent to the terms and conditions expressly… [a] party instead gives his assent simply by using the website." *Southwest Airlines Co. v Boardfirst, LLC* (ND Tex, Sept. 12, 2007, No. 3: 06-CV-0891-B) 2007 US Dist Lexis 96230 at *14. Users are expected to find and review the text of the documents on their own. Typically, the website or the document itself includes a statement that a user's continued use of the website or the software downloaded from the site evidences the user's agreement to all of the terms and conditions of the document.

In ruling on the validity of browse-wrap agreements, courts consider primarily "whether a website user has actual or constructive knowledge of a site's terms and conditions prior to using the site." *Hines v Overstock.com, Inc*. (ED NY, Sept. 8, 2009, No. 09 CV 991) 2009 US Dist Lexis 81204 at *6, quoting *Southwest Airlines Co. v Boardfirst, LLC,* 2007 US Dist Lexis 96230 at *15. See also *Specht v Communications Netscape Communications Corp.* (2d Cir 2002) 306 F3d 17, 20. Several courts that have considered browse-wrap agreements have been reluctant to enforce them because of their noninteractive nature. See, *e.g., Ticketmaster Corp. v Tickets.com, Inc.* (CD Cal, Mar. 7, 2003, CV99-7654 HLH) 2003 US Dist Lexis 6483, and the earlier decision in the same case, *Ticketmaster Corp. v Tickets.com, Inc.* (CD Cal, Mar. 27, 2000, CV99-7654 HLH) 2000 US Dist Lexis 4553.

In *Ticketmaster Corp. v Tickets.com, Inc., supra*, Ticketmaster claimed that Tickets.com's use of so-called "spiders" (a specialized type of web-based automated search software) violated Ticketmaster's terms of use, which prohibited such activity. The "spiders" located event listings on Ticketmaster's website. Tickets.com used this information for commercial purposes on its own website by inserting "deep links" to interior pages of Ticketmaster's website, enabling end users to bypass the Ticketmaster home page and directly access the desired event listing. Ticketmaster's home page included a prominent notice stating that, by proceeding beyond the home page to interior pages of the website, users accepted Ticketmaster's terms of use, and the court found that Tickets.com was aware of the notice. The court acknowledged that a binding contract on the Internet could be formed without requiring a user to separately click "I agree." The court ruled that "a contract can be formed by proceeding into the interior web pages after knowledge (or, in some cases, presumptive knowledge) of the conditions accepted when doing so." 2003 US Dist Lexis 6483 at 9. See also the previous decision in this case, *Ticketmaster Corp. v Tickets.com, Inc.* (CD Cal, Mar. 27, 2000, CV99-7654 HLH) 2000 US Dist Lexis 4553, in which the court held that merely posting terms and conditions on a website does not create a contract with a user of the website unless it can be established that the user had actual knowledge of the contract terms. For additional discussion of the *Ticketmaster* litigation, see §18.21.

Both *Ticketmaster* decisions highlight the importance of placing terms of use or other browse-wrap agreements in a conspicuous and readily accessible part of the website. The reasoning in these cases indicates that courts will require both *notice* (*i.e.,* making online agreements conspicuous to site users) and *proof* that a user actually accessed the online agreement before enforcing the agreement. The more action required on the part of the website user, the more likely a court will hold that a contract has been formed. Compare the *Ticketmaster* decisions with *Pollstar v Gigmania* (ED Cal 2000) 170 F Supp 2d 974, in which the court refused to enforce the terms of an online license agreement because the link to it was not sufficiently obvious. The *Pollstar* court did not rule that the license agreement was per se unenforceable, only that the website did not give users adequate notice of it. In *Specht v Netscape Communications Corp.* (2d Cir 2002) 306 F3d 17, the Second Circuit refused to enforce an arbitration clause contained in a browse-wrap software license agreement because end users were able to download the free software without reviewing the license agreement: To view the license terms, users were required to scroll down below the "download" button and click on a hyperlink. At no time were users required to indicate their agreement to those terms. The court held that (306 F3d at 30):

[A] reasonably prudent Internet user in circumstances such as these would not have known or learned of the existence of the license terms before responding to defendants' invitation to download the free software, and that defendants therefore did not provide reasonable notice of the license terms. In consequence, plaintiffs' bare act of downloading the software did not unambiguously manifest assent to the arbitration provision contained in the license terms.

The Second Circuit rejected Netscape's argument that the plaintiffs had "inquiry notice" of the terms of the license, and affirmed the lower court's decision that plaintiffs neither had reasonable notice of the existence of the license terms nor manifested unambiguous assent to those terms before acting on the website's invitation to download the software. The *Specht* court also noted that the Uniform Computer Information Transactions Act (see §7.11) includes a provision requiring websites to display noninteractive terms in a prominent and conspicuous manner so that website users would be on notice that their use of the site was subject to those terms. See 306 F3d at 34.

PRACTICE TIP: Both *Pollstar* and *Specht* serve as cautions to website operators who might prefer not to require their users to confront click-wrap agreements before accessing website content. Failure to require users to review and affirmatively accept the terms of use may result in a court's refusal to enforce those terms if the court finds that users do not have sufficient notice of them.

In *Hines v Overstock.com, Inc.* (ED NY, Sept. 8, 2009, No. 09 CV 991) 2009 US Dist Lexis 81204, the court found that the plaintiff had no actual or constructive notice of Overstock.com's terms and conditions, or the arbitration provision included in those terms, when she filed a class action regarding restocking fees imposed by Overstock.com in connection with product returns. The terms were only referenced in a hyperlink in small type on the bottom of the Overstock.com website and plaintiff "was never advised of the Terms and Conditions and could not even see the link to them without scrolling down to the bottom of the screen." 2009 US Dist Lexis 81204 at 8.

PRACTICE TIP: The more interactive a site is—for example, if users can conduct transactions on the site—the more important it becomes to require affirmative assent to website terms to bolster the site operator's ability to enforce those terms.

In a commercial context, however, courts have been more inclined to find terms of use binding on the end user of an Internet site. In *Register.com, Inc. v Verio, Inc.* (2d Cir 2004) 356 F3d 393, the court found Verio's repeated use of Register.com's WHOIS database evidence of consent to Register.com's terms of use, notwithstanding that Verio did not see the terms of use until after it had finished using the database and did not click on an "I agree" button indicating its agreement to be bound. Verio obtained information from the Register.com database through the use of a "robot" (an automated tool used to gather information on the Internet, also known as a "crawler") and then used the information, in violation of Register.com's terms of use, to solicit business. Repeated use of the site, with knowledge of the existence of such terms of use, was enough to convince the court that Verio should be bound by them.

Similarly, the court in *Ticketmaster LLC v RMG Technols., Inc.* (CD Cal 2007) 507 F Supp 2d 1096, 1107, upheld the Ticketmaster browse-wrap agreement, which prohibited the use of "automated devices" to access its site and copy or use its pages for commercial purposes. RMG markets and sells applications that enable its clients to use automated devices to enter and navigate through third party websites. Ticketmaster claimed that RMG's application circumvented its access control and copy protection systems, inundated Ticketmaster's computers with thousands of automatic requests, prevented ordinary consumers from accessing the website, and enabled RMG's clients to purchase large quantities of tickets. 507 F Supp 2d at 1102. The court found that defendant's use of the Ticketmaster website constituted acceptance of the Ticketmaster terms of use. 507 F Supp 2d at 1108. See also *Treiber & Straub, Inc. v UPS, Inc.* (7th Cir 2007) 474 F3d 379 (restrictions on value of goods to be shipped contained in website "Terms and Conditions" constituted notice adequate to preclude insurance recovery); *Southwest Airlines Co. v Boardfirst, LLC* (ND Tex, Sept. 12, 2007, No. 3: 06-CV-0891-B) 2007 US Dist Lexis 96230 (Boardfirst's use of the Southwest website to assist customers in obtaining boarding passes issued on a "first come, first served" basis for fee was commercial use in violation of website's terms of use); *Cairo, Inc. v CrossMedia Servs., Inc.* (ND Cal, Apr. 1, 2005, No. C04-04825) 2005 US Dist Lexis 8450 (website terms of use binding given actual knowledge of terms, continued use of site, and imputed knowledge of terms resulting from repeated robot access to database).

In a consumer context, the Third Circuit ruled against a subscriber to cable Internet service who claimed he was unaware of the agreement governing his subscription, including his obligation to arbitrate disputes with the provider. *Schwartz v Comcast Corp.* (3d Cir 2007) 256 Fed Appx 515 (unpublished). The subscriber claimed he had never agreed to the terms of the subscriber agreement, or had even been provided with one upon subscribing. The court rejected his claim, reasoning that it was the provider's "consistent practice" to deliver subscription agreements to subscribers, that the agreement was available on the provider's website, and that the subscriber paid the bill for the service provided, thus performing in accordance with the subscription agreement's terms.

Some online commercial browse-wrap agreements contain embedded links to other documents or policies that are incorporated by reference. In *PDC Labs., Inc. v Hach Co.* (CD Ill, Aug. 25, 2009, No. 09-1110) 2009 US Dist Lexis 75378, the court held that a limitation of damages clause in a commercial agreement was not procedurally unconscionable and was therefore enforceable, despite the fact that it was only readable by clicking through a hyperlink embedded in the terms and conditions. The court found that the hyperlink, underlined and shown in a contrasting blue, was sufficiently conspicuous. 2009 US Dist Lexis 75378 at 8.

© The Regents of the University of California

III. E-SIGN

§7.5 A. Introduction

The Electronic Signatures in Global and National Commerce Act (E-Sign) (15 USC §§7001-7031) confirms the ability of parties to contract electronically, defining an "electronic signature" broadly as "an electronic sound, symbol or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." 15 USC §7006(5). See §7.6. This definition encompasses click-wrap agreements (see §7.3), thus assuring their enforceability. E-Sign provides that any signature, contract, or other record cannot be denied legal effect, validity, or enforceability solely because it is in electronic form (15 USC §7001(a)(1)), and any contract cannot be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation (15 USC §7001(a)(2)). E-Sign, however, does not require any person to agree to use or accept electronic records or electronic signatures. 15 USC §7001(b)(2).

© The Regents of the University of California

§7.6 B. Electronic Signatures

At common law, any symbol made with the intent to sign a document could qualify as a legally valid signature. The definition of "signed" in the Uniform Commercial Code includes "any symbol," as long as it is "executed or adopted with present intention to adopt or accept a writing." UCC §1-201(37). See also Comment 37 to Com C §1201. E-Sign extends this approach to electronic signatures by requiring that an electronic signature possess three elements (15 USC §7006(5)):

- A sound, symbol, or process,
- Attached to or logically associated with an electronic record, and
- Made with the intent to sign the electronic record.

An electronic signature can take many forms, and can be created by many different technologies. Examples of electronic signatures that should qualify under E-Sign include:

- Typing the sender's name at the end of an e-mail message sent by him or her;
- Including a digitized image of a handwritten signature attached to an electronic document;
- A mouse click (*e.g.,* on an "I accept" or "I agree" button); and
- A "digital signature" (*e.g.,* a signature created through public key cryptography).

PRACTICE TIP: A New York court held that a series of e-mails were "signed" writings sufficient to modify an employment agreement that contained a clause requiring all amendments to be signed. *Stevens v Publicis* (App Div 2008) 854 NYS2d 690. Given the apparent trend toward a liberal interpretation of what it means for a party to have "signed" something, counsel should consider whether a contract should specify that a typed name or exchange of e-mails is not sufficient to satisfy the requirement that any amendment must be signed by the parties.

© The Regents of the University of California

§7.7 C. Consumer Protection Features

In addition to granting legal effect to electronic documents generally, E-Sign includes several provisions intended to protect the rights of consumers in electronic transactions. E-Sign's consumer protection provisions are triggered only when a statute, regulation, or other rule of law requires that information relating to a transaction be provided or made available to a consumer in writing. 15 USC §7001(c). Providing information electronically in these circumstances is acceptable only if the consumer affirmatively consents to receive the information in electronic form, gives his or her consent electronically, and does so in a manner that reasonably demonstrates that he or she can access the information in the electronic format that will be used to provide it. 15 USC §7001(c)(1)(A), (c)(1)(C)(ii).

Before giving consent, the consumer must receive a clear and conspicuous statement of his or her rights, the scope of the consent given, and how to withdraw the consent. 15 USC §7001(c). In particular, businesses are required to take the following actions:

- Inform the consumer of (1) any right to have an electronic record made available in nonelectronic (paper) form, (2) the right of a consumer to withdraw his or her consent to have the record provided in an electronic form, and (3) any conditions, consequences (such as termination of the parties' relationship), or fees if the consumer's consent is withdrawn (15 USC §7001(c)(1)(B)(i));

- Inform the consumer whether his or her consent applies (1) only to the specific transaction that gave rise to the obligation to provide the record, or (2) to identified categories of records that may be provided over the course of the parties' relationship (15 USC §7001(c)(1)(B)(ii));

- Describe the procedures the consumer is required to use to withdraw consent and to update information needed to contact the consumer electronically (15 USC §7001(c)(1)(B)(iii));

- Inform the consumer of (1) how, after consenting to the electronic record, the consumer may obtain a paper copy of the electronic record on request, and (2) the fee, if any, to be charged for such copy (15 USC §7001(c)(1)(B)(iv));

- Provide the consumer (before consent) with a description of the hardware and software requirements for access to and retention of the electronic records (15 USC §7001(c)(1)(C)(i)); and

- If the software or hardware requirements necessary to access the electronic record change, advise the consumer of (1) the new hardware and software requirements, and (2) the consumer's right to withdraw consent without the imposition of any fees or any condition or consequence not previously disclosed (15 USC §7001(c)(1)(D)(i)).

© The Regents of the University of California

§7.8 D. Electronic Record Retention

Under E-Sign, if the law requires that a record of a contract be retained, an electronic record is adequate for the purpose, provided that it "accurately reflects the information" in the contract and the record remains accessible for later reference in a form that can be accurately reproduced. 15 USC §7001(d)(1). E-Sign provides that the legal effect, validity, or enforceability of an electronic record "may be denied if such electronic record is not in a form that is capable of being retained and accurately reproduced for later reference by all parties or persons who are entitled to retain the contract or other record." 15 USC §7001(e). Even if a contract is not required by law to be retained, it is always advisable to keep a record of an electronic contract for evidentiary purposes. Thus, a website operator should include online functionalities for printing and saving electronic agreements to better assure their enforceability.

NOTE: Courts may decline to enforce an agreement allegedly agreed to electronically, absent competent evidence of a party's assent to its terms. In *FTC v Cleverlink Trading Ltd.* (ND Ill 2007) 519 F Supp 2d 784, 795 (applying Illinois law) the party seeking to recover fees pursuant to an unsigned Merchant Payment Process Services Agreement (MPPSA) it submitted to the court, claimed the other party had agreed electronically to the MPPSA's terms. The court deemed the sole evidence submitted in support of that claim—an e-mail comprising a line of computer code which the court found undecipherable—inadequate to prove agreement to the MPPSA's terms.

© The Regents of the University of California

IV. UNIFORM ELECTRONIC TRANSACTIONS ACT (UETA)

§7.9 A. Overview

Before E-Sign, California adopted a version of the Uniform Electronic Transactions Act (UETA) (see CC §§1633.1-1633.17), which applies to transactions between parties who have each agreed to conduct a transaction electronically. UETA provides for the enforceability of electronic contracts, as well as for records retention and the evidentiary use of electronic records. As of this writing, almost all states have adopted a version of UETA. See http://www.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fs-ueta.asp. Although broader than E-Sign, UETA covers many of the same issues as E-Sign and is therefore subject to federal preemption. E-Sign, however, has an exemption from federal preemption applicable in states where UETA has been enacted in the form recommended by the National Conference of Commissioners on Uniform State Laws (NCCUSL). The California version of UETA is nonconforming; it substantially altered many of UETA's provisions. Under E-Sign, however, only provisions that would create an exception to the scope of UETA (as recommended by NCCUSL) and are otherwise inconsistent with E-Sign are subject to federal preemption by E-Sign. See 15 USC §7002. Thus, the scope of E-Sign's potential preemption of California's version of UETA is unclear. It is therefore advisable to assume that E-Sign's restrictions and exclusions will apply in California and any other state that has not enacted UETA in the form recommended by NCCUSL.

© The Regents of the University of California

§7.10 B. Consent Under UETA

Both E-Sign and Uniform Electronic Transactions Act (UETA) authorize parties to enter into electronic transactions, but do not require parties to do so. See 15 USC §7001(b)(2); CC §1633.5(a). Unlike E-Sign, UETA is premised on consent by the parties; the statute does not apply unless the parties have "agreed to conduct transactions by electronic means." CC §1633.5(b). The consent requirement applies to both business and consumer transactions. Whether the parties have consented to conduct a transaction by electronic means is determined from the context and circumstances surrounding the transaction, and consent may be either express or implied. CC §1633.5(b). Under the California version of UETA, consent must be given by electronic means. CC §1633.5(b). If a company's website is capable of receiving electronic communications from customers, and a customer enters into a transaction with the company using the company's website, it can be inferred that both parties have impliedly agreed to conduct their transaction electronically.

© The Regents of the University of California

§7.11 V. UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT (UCITA)

The Uniform Computer Information Transactions Act (UCITA) has been an effort spearheaded by the software industry to develop uniform state legislation with default rules for the creation and enforcement of contracts (including shrink-wrap and click-wrap licenses) relating to electronic information. For example, it would cover agreements for the development, distribution, licensing, and transfer of computer software, multimedia products, computer databases, and Internet websites. The full text of the model uniform law is posted at http://www.law.upenn.edu/bll/ulc/ucita/2002final.htm. UCITA was patterned in part after Article 2 of the Uniform Commercial Code and was intended to fill the gap in coverage of the UCC that exists because Article 2 ostensibly applies only to tangible goods and not to intangible property, such as software. For the most part, UCITA attempted to codify practices already in use with respect to computer information and supported freedom of contract. Among other things, UCITA set uniform guidelines for shrink-wrap, click-wrap, and browse-wrap agreements, making it clear that such agreements would be legally binding as long as the user has an opportunity to review the terms before assenting.

To date, only two states, Virginia and Maryland, have adopted UCITA. See Va Code Ann §59.1-501.1—59.1-509.2; Md Comm Law C Ann §22-101—22-816. UCITA, however, provides that companies based in a state that has not adopted UCITA may elect to have their contracts governed by the laws of a state that has adopted it. For example, a consumer in Alaska could purchase software issued by a California company and discover that the shrink-wrap license inside the package purports to be governed by Virginia law—and therefore UCITA.

UCITA has proved to be extremely controversial and has been opposed by various interest groups because of its perceived unfairness to consumers, alleged conflicts with federal copyright law, and other reasons. See, *e.g.*, http://www.ucita.com. Four states to date—Iowa, North Carolina, Vermont, and West Virginia—have adopted so-called "bomb shelter" (anti-UCITA) legislation that protects software licensees from choice-of-law provisions making UCITA the governing law of the contract or from choice-of-forum provisions that select a state unrelated to either the licensee or the vendor as the forum for settling legal disputes under the contract.

California has not yet adopted UCITA, and UCITA's future is presently uncertain. In the summer of 2003, citing widespread opposition from consumers, libraries, and other interest groups, the National Conference of Commissioners on Uniform State Laws pulled its support for the legislation, announcing that it would not seek its adoption in any other state. Because UCITA is the law in Maryland and Virginia, however, and because it has served as a resource for judges in cases relating to electronic information, the controversy will likely continue.

PRACTICE TIP: California practitioners should be generally familiar with the scope of UCITA, even though it has not been adopted in this state. If the parties to a contract for software or other electronic information do not wish UCITA to apply in interpretation or enforcement of the agreement, the parties should affirmatively disclaim its applicability in the text of the agreement. For an example of such a disclaimer, see Section 11 of the form of Software Development Agreement in §13.3.

© The Regents of the University of California

§7.12 VI. ALI SOFTWARE CONTRACT PRINCIPLES

On May 19, 2009, the American Law Institute (ALI) approved the Proposed Final Draft, dated March 16, 2009, of the Principles of the Law of Software Contracts (Principles), copies of which are available for purchase at http://www.ali.org/index.cfm?fuseaction=publications.ppage&node_id=121. According to the Introduction, the Principles "seek to clarify and unify the law of software transactions" (Principles at 2) in view of (1) the failure of the Uniform Computer Information Transactions Act (UCITA) to win general acceptance and (2) the general inapplicability of Article 2 of the Uniform Commercial Code to software transactions. The Principles were not intended to be a restatement of the law, but rather to "account[] for the case law and recommend[] best practices." (Principles at 2). The Introduction clarifies that the Principles "are not the law unless and until a court adopts [them]. Courts can apply the Principles as definitive rules, as a 'gloss' on the common law, U.C.C. Article 2, or other statutes, or not at all as they see fit." Principles at 2.

The Principles consist of 31 separate sections with accompanying comments, divided into four chapters addressing many topics, as follows:

- **Chapter 1:** Definitions, scope, and general terms (including provisions on unconscionability, choice of law, and choice of forum).
- **Chapter 2:** Formation and enforcement (including provisions on standard-form transfers of generally available software, enforcement of the standard form, and contract modification).
- **Chapter 3:** Performance (including provisions concerning implied indemnification, express and implied warranties, the parol-evidence rule and its interpretation, and breach).
- **Chapter 4:** Remedies (including provisions on agreements to modify or limit remedies, liquidated damages, use of automatic disablement to impair use, and remedies in the absence of agreement).

The Principles are intended to apply to agreements for transfer of software for consideration, including agreements to sell, lease, license, access, or otherwise transfer or share software. Principles §1.06(a). The Principles do not cover digital art, databases, or other media content; do not cover security interests (Comment a to Principles §1.06); and may or may not cover embedded software depending on the circumstances (Principles §1.07).

A detailed analysis of the Principles is beyond the scope of this chapter, but one particularly controversial provision bears noting. Section 3.05(b) sets forth a purportedly nondisclaimable implied warranty that a transferor that receives money or a right to payment in money in exchange for software warrants "to any party in the normal chain of distribution that the software contains no material hidden defects of which the transferor was aware at the time of the transfer." Both Microsoft Corporation and the Linux Foundation, along with other software licensors, objected to §3.05(b) as likely to provoke significant litigation without benefiting licensees. Many forms of software license agreement now include blanket disclaimers of the applicability of UCITA to the transaction. At least until there is some judicial clarification of the Principles in reported case decisions, counsel for software licensors may consider including disclaimers of the applicability of the Principles in their form agreements.

© The Regents of the University of California

§7.13 VII. EUROPEAN UNION DIRECTIVES

In the European Union, the enforceability of electronic transactions is governed by both the Electronic Signatures Directive (ES Directive), which was adopted in 1999 (Directive 1999/93/EC of 13 December 1999 (http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML)), and the Electronic Commerce Directive (EC Directive), adopted in 2000 (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 (http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML)). The European Union ES Directive requires member states to "ensure that an electronic signature is not denied legal effectiveness … solely on the grounds that it is in electronic form." ES Directive, Art 5(2).

© The Regents of the University of California

§7.14 VIII. CREATING ENFORCEABLE ELECTRONIC AGREEMENTS

Although E-Sign, the Uniform Electronic Transactions Act (UETA), and recent case decisions make it probable that click-wrap agreements will be enforced, counsel should take steps to assure that click-wrap and other electronic agreements conform with applicable statutes and case law. In the wake of the lower court's decision in *Specht v Netscape Communications Corp.* (SD NY 2001) 150 F Supp 2d 585, aff'd (2d Cir 2002) 306 F3d 17 (see §7.4), an American Bar Association working group convened to assess strategies for creating enforceable click-wrap agreements, ultimately recommending the following six principles as guidance for structuring and implementing online agreements (see Kunz, *Click-Through Agreements: Strategies for Avoiding Disputes on Validity of Assent*, 57 Bus Law 401 (2001)):

- Users should have easy, automatic access to the terms of the agreement, as well as a subsequent opportunity to review the terms;
- Contract terms should be displayed in a way that complies with applicable laws on format and content, such as laws governing notice, disclosure, and conspicuousness;
- Users should be required to take affirmative action to indicate their assent to the contract terms and should be informed of the consequences of clicking on the "I Agree" button;
- Users should be given a clear means by which they can reject the proposed terms, and should be informed of the consequences of rejecting the agreement terms;
- The agreement process should include a method for users to avoid, or to detect and correct, errors likely to be made by the user; and
- Users should be able to print out a version of the agreement terms, and software vendors should have a method for preserving records of the agreed-to terms and of the manner in which users indicated assent to those terms.

Practitioners should also take heed of these additional practical considerations:

- The contract should include a representation or warranty covering the identity and authority of the user accepting the contract—that they are who say they are, and if they are entering the contract on behalf of another person or entity, that they have authority to bind that other person or entity.
- It may be appropriate to include a representation and warranty that the contracting party is an adult (over a specified age), capable of entering into a binding agreement, and not a minor.
- The contract will be interpreted under traditional contract law principles. Accordingly, it is important to observe the same rules that would apply to a "paper" contract. If a term or condition would not be enforceable offline, it will not be enforceable online. Courts will reject any terms that they deem unreasonable or unconscionable, based on the facts and circumstances of each case.
- The click-wrap agreement should not contains terms that might be considered unreasonable or unfair or that might surprise an average software consumer. Terms that might be viewed as overly harsh or one-sided include arbitration clauses, forum selection clauses, and limitations on liability for damages. See, *e.g.*, *Brazil v Dell Inc.* (ND Cal, Aug. 3, 2007, No. C-07-01700 RMW) 2007 US Dist Lexis 59095 (arbitration clause in click-wrap agreement for purchase of computer equipment held unenforceable); *Aral v EarthLink, Inc.* (2005) 134 CA4th 544, 36 CR 3d 229 (California court struck arbitration clause in browse-wrap DSL agreement that required subscribers to travel to Georgia to obtain redress).
- Online software purchasers should be notified that use of the software is subject to the terms of the vendor's license agreement and that the vendor will not enter into the transaction unless that purchaser agrees to its terms.
- The user should be required to review and accept the license agreement before payment and delivery of the software, so that the license agreement forms an integral part of the transaction. Software distributors should thereby avoid the problems faced by the vendor in *Step-Saver Data Sys. v Wyse Technol.* (3d Cir 1991) 939 F2d 91 (relying on former UCC §2-207(2)(b), court found that disclaimer of warranty and limitation of remedies in box-top software license delivered after purchase contract was formed had never been accepted by purchaser).

- The purchaser should be required to review the entire agreement before accepting it and to expressly assent to the terms by taking some affirmative action, such as clicking on an "Accept" or "I Agree" button before the software can be downloaded.

- Buttons or icons for "I Agree" and "I Do Not Agree" should be placed at the end of the terms of an online contract, along with statements indicating (1) the effect of clicking on "I Agree" (*e.g.,* "These terms will form a binding legal contract between us as soon as you click the 'I Agree' button."), and (2) the effect of clicking on "I Do Not Agree" (*e.g.,* "If you do not agree to accept these terms, click 'I Do Not Agree' below, and you will not be permitted to install or use this software.").

- When users are presented with choices or are asked to furnish information in connection with their agreement to an online contract, users should also be asked to review those choices (or information furnished) on a confirmation screen and be given a chance to correct any errors before assenting to the contract.

Many electronic agreements include language permitting the modification of the agreement unilaterally by the website owner. In some situations, e-mail notice of the amendment is provided to the end user. In such situations, care should be taken to put the recipient of the e-mail on notice of the importance of the message in the e-mail's subject line. In *Campbell v General Dynamics Gov't Sys. Corp.* (D Mass 2004) 321 F Supp 2d 142, 144, the court refused to enforce an arbitration policy because notice of adoption of the policy, contained in a single e-mail, was insufficient. No information in the subject line indicated that the message was critically important, the message was addressed not to an individual but to a "fellow employee," and nothing in the message's opening paragraphs suggested that the message pertained to employees' legal rights. See also *Marlar v Yellow Transp.* (WD Mo, Nov. 29, 2004, No. 03-1042-CV-W-HFS) 2004 US Dist Lexis 26653, *21 (electronic notice held adequate when e-mail heading clearly indicated adoption of new procedures, used bold type for emphasis, and stated date after which employment would be conditioned on acceptance of new procedures).

In *Douglas v District Court* (9th Cir 2007) 495 F3d 1062, the service provider posted amendments to a contract for long distance telephone service on its website without any notice to users. The changes included additional service charges, a class action waiver, an arbitration clause, and a choice-of-law provision opting for New York law. 495 F3d at 1065. The court held the modifications ineffective where the notice of the changed terms consisted only of posting the revised contract on the service provider's website. 495 F3d at 1067.

Some website owners state that their terms of use are subject to modification unilaterally from time to time without notice or with notice only posted on the website itself. In *Harris v Blockbuster Inc.* (ND Tex 2009) 622 F Supp 2d 396, the court held the arbitration clause found in the Blockbuster online terms of use to be illusory and therefore unenforceable because Blockbuster maintained the right to modify its terms and conditions unilaterally at any time. 622 F Supp 2d at 399. The court suggested, however, that it would view the situation differently if the terms provided a "savings clause" making the changes to the arbitration clause applicable prospectively and not retroactively. 622 F Supp 2d at 399.

PRACTICE TIP: While on its face the *Blockbuster* ruling may appear to have narrow application, dicta in *Blockbuster* suggests that its holding may apply to the online service terms as well as the arbitration clause. 622 F Supp 2d at 400. Therefore, when drafting website terms of use, consider adding language stating that an amendment is effective beginning on the date it is posted, and that amended dispute resolution terms do not apply to any dispute of which the parties had actual notice before the date of the amendment.

When amendments are intended to apply retroactively, the FTC has taken the position in at least one case that opt-in consent of affected end users is required. *In re Gateway Learning Corp.* (July 7, 2004) FTC File No. 042-3047, available at http://www.ftc.gov/os/caselist/0423047/040707agree042347.pdf.

© The Regents of the University of California

8

Terms of Use; Online Agreements; Linking; Downloading

I. INTRODUCTION §8.1

II. TERMS OF USE
- A. Generally §8.2
- B. Form: Website Terms of Use §8.3

III. ONLINE SOFTWARE LICENSE AGREEMENTS
- A. Introduction §8.4
- B. Form: Online End-User Software License Agreement §8.5
- C. Online Beta User Evaluation Agreement
  - 1. Introduction §8.6
  - 2. Form: Online Beta User Evaluation Agreement §8.7
- D. Open Source Licensing
  - 1. Introduction §8.8
  - 2. Form: Open Source Software License Agreement §8.9
- E. Software Evaluation License Agreement
  - 1. Introduction §8.10
  - 2. Form: Evaluation License Agreement §8.11
- F. Online Software Developer Toolkit License Agreement
  - 1. Introduction §8.12
  - 2. Form: Online Software Developer Toolkit License Agreement §8.13

IV. LINKING ARRANGEMENTS
- A. Introduction §8.14
- B. Linking and Framing
  - 1. Generally §8.15
  - 2. Copyright Infringement Issues §8.16
  - 3. Potential Liability for Trespass to Chattels §8.17
- C. Form: Linking Agreement §8.18

V. DOWNLOADING AND UPLOADING CONTENT
- A. Generally §8.19
- B. Copyright Infringement Issues §8.20
- C. Music on the Internet
  - 1. Introduction §8.21
  - 2. Technologies §8.22
  - 3. Federal Statutes §8.23
    - a. Audio Home Recording Act of 1992 (AHRA) §8.24
    - b. Digital Performance Right in Sound Recordings Act of 1995 (DPRA) §8.25
    - c. No Electronic Theft Law §8.26
    - d. Internet Piracy (Pen C §653aa) §8.26A
    - e. The Family Entertainment and Copyright Act §8.26B
  - 4. Case Law §8.27
  - 5. RIAA Litigation Strategy §8.28

© The Regents of the University of California

§8.1 I. INTRODUCTION

This chapter addresses a variety of ways in which Internet users interact with websites, including contracts between users and website sponsors relating to such interaction, and selected legal issues that may arise in this context. Section 8.2 discusses terms of use—company policies intended to control website usage by customers, typically accessible by a link at the bottom of a company's home page. A model form of terms of use is set forth and analyzed in §8.3. Sections 8.4-8.12 examine several different types of online software license agreements, including an agreement to govern end use of downloaded software, an agreement for testing and evaluation of a software program, and several agreements relating to online software development. Sections 8.14-8.18 discuss linking arrangements, and include a form of linking agreement. Finally, §§8.19-8.24 address issues relating to downloading and uploading of the content of Internet websites, including music.

Website privacy policies and applicable privacy laws are discussed in chap 9.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/8 Terms of Use; Online Agreements; Linking; Downloading/ II. TERMS OF USE/§8.2 A. Generally

II. TERMS OF USE

§8.2 A. Generally

Terms of use are intended to govern the use of the company's website, network, or systems by customers or external users. Terms of use typically include the following provisions, among others:

- A description of the services provided;
- An ownership claim with respect to intellectual property included as part of the service;
- The grant of a license to users covering the intellectual property necessary for them to use the service;
- The grant of a license from a user to the company for the company's use of any intellectual property provided by the user as part of the user's use of the service;
- A clause specifying whether or not users are allowed to link to the service, and if so, specifying any restrictions on such linking; and
- A prohibition on users violating any laws, regulations, or company policies, or performing any other actions that the company wishes to prohibit.

In addition, the terms of use should include an explanation of the company's monitoring policy and a requirement that the user consent to such monitoring as a condition of access to the website, network, systems, or services. The terms of use should also specify the exclusive choice of forum and choice of law to govern any conflicts arising from use of the website, network, or systems of the company. See generally chap 19.

Under the Digital Millennium Copyright Act (17 USC §§512, 1201-1332), more fully discussed in §§1.24-1.43), a website's terms of use should include the name, address, telephone number, e-mail address, and other contact information for a person designated by the company to receive notices under 17 USC §512(c) or (d) of copyright infringement claims. See §§1.37-1.38, 1.40.

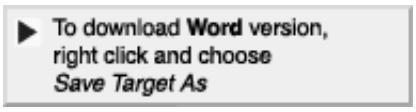
A company normally intends that its terms of use constitute a binding contract between the company and users of its website. Yet many terms of use policies are simply posted on websites and made accessible through a hyperlink without requiring the user to formally indicate acceptance of the terms before using the website. Terms of use that do not require a user to take specific action to consent to the terms, such as clicking an "I Agree" button, are known as "browse-wrap" agreements and may or may not be enforceable.

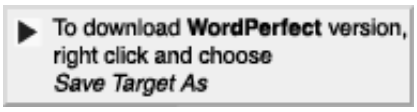
PRACTICE TIP: Before drafting terms of use for a website, counsel should review the considerations outlined in §7.13 for creating enforceable electronic agreements. An increasing number of reported cases have considered the enforceability of browse-wrap and other online agreements. On electronic contracting generally, see chap 7.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/8 Terms of Use; Online Agreements; Linking; Downloading/§8.3 B. Form: Website Terms of Use

§8.3 B. Form: Website Terms of Use





TERMS OF USE OF _ _[*NAME OF WEBSITE OR SERVICE PROVIDER*]**_ _**

1. BINDING EFFECT. This is a binding agreement. By using the Internet site located at _ _[*specify website address*]**_ _ (the "Site") or any services provided in connection with the Site (the "Service"), you agree to abide by these Terms of Use, as they may be amended by _ _**[*name of service provider*]**_ _ ("Company") from time to time in its sole discretion. Company will post a notice on the Site any time these Terms of Use have been changed or otherwise updated. It is your responsibility to review these Terms of Use periodically, and if at any time you find these Terms of Use unacceptable, you must immediately leave the Site and cease all use of the Service and the Site. YOU AGREE THAT BY USING THE SERVICE YOU REPRESENT THAT YOU ARE AT LEAST 18 YEARS OLD AND THAT YOU ARE LEGALLY ABLE TO ENTER INTO THIS AGREEMENT.**

Comment: Note that notice of an amendment to a website's terms of use should be provided to end users either by e-mail (if users must register and provide e-mail in order to use the site) or by posting a conspicuous notice on the website itself. The site operator should either post clear descriptions of the modifications made or show the user the changes by using a highlighted version of the terms, or both. Merely requiring the end user to compare previous and revised versions on his or her own may not be sufficient to result in a binding amendment. If the website provides a service but users do not routinely access the site itself in order to use the service (such as a software subscription, where fees are payable monthly but the user only needed to access the site for the initial download of the software), it may not be reasonable to assume that notice posted on the site is sufficient. See *Douglas v District Court* (9th Cir 2007) 495 F3d 1062. See §7.4.

2. PRIVACY POLICY. Company respects your privacy and permits you to control the treatment of your personal information. A complete statement of Company's current privacy policy can be found by clicking here. Company's privacy policy is expressly incorporated into this Agreement by this reference.

Comment: If users are assigned an account or password for use of the website or service, consider adding a provision regarding confidentiality and security of such passwords, as follows:

> **When you are required to open an account to use or access the Site or Service, you must complete the registration process by providing the complete and accurate information requested on the registration form. You will also be asked to provide a user name and password. You are entirely responsible for maintaining the confidentiality of your password. You may not use the account, username, or password of someone else at any time. You agree to notify Company immediately on any unauthorized use of your account, user name, or password. Company shall not be liable for any loss that you incur as a result of someone else using your password, either with or without your knowledge. You may be held liable for any losses incurred by Company, its affiliates, officers, directors, employees, consultants, agents, and representatives due to someone else's use of your account or password.**

See chap 9 for a sample privacy policy and a discussion of the law applicable to personally identifiable information collected or maintained online.

3. USE OF SOFTWARE. Company may make certain software available to you from the Site. If you download software from the Site, the software, including all files and images contained in or generated by the software, and accompanying data (collectively, "Software") are deemed to be licensed to you by Company, for your personal, noncommercial, home use only. Company does not transfer either the title or the intellectual property rights to the Software, and Company retains full and complete title to the Software as well as all intellectual property rights therein. You may not sell, redistribute, or reproduce the Software, nor may you decompile, reverse-engineer, disassemble, or otherwise convert the Software to a human-perceivable form. All trademarks and logos are owned by Company or its licensors and you may not copy or use them in any manner.

Comment: Consider adding language granting or restricting the right of users to link to the website or the service, or reserving the right to disable links from third party sites to the website. Depending on the client and the services provided, consider adding language prohibiting users from performing meta-searches of the website or the service, or sending automated queries to the website or the service.

4. USER CONTENT. You grant Company a license to use the materials you post to the Site or Service. By posting, downloading, displaying, performing, transmitting, or otherwise distributing information or other content ("User Content") to the Site or Service, you are granting Company, its affiliates, officers, directors, employees, consultants, agents, and representatives a license to use User Content in connection with the operation of the Internet business of Company, its affiliates, officers, directors, employees, consultants, agents, and representatives, including without limitation, a right to copy, distribute, transmit, publicly display, publicly perform, reproduce, edit, translate, and reformat User Content. You will not be compensated for any User Content. You agree that Company may publish or otherwise disclose your name in connection with your User Content. By posting User Content on the Site or Service, you warrant and represent that you own the rights to the User Content or are otherwise authorized to post, distribute, display, perform, transmit, or otherwise distribute User Content.

5. COMPLIANCE WITH INTELLECTUAL PROPERTY LAWS. When accessing the Site or using the Service, you agree to obey the law and to respect the intellectual property rights of others. Your use of the Service and the Site is at all times governed by and subject to laws regarding copyright ownership and use of intellectual property. You agree not to upload, download, display, perform, transmit, or otherwise distribute any information or content (collectively, "Content") in violation of any third party's copyrights, trademarks, or other intellectual property or proprietary rights. You agree to abide by laws regarding copyright ownership and use of intellectual property, and you shall be solely responsible for any violations of any relevant laws and for any infringements of third party rights caused by any Content you provide or transmit, or that is provided or transmitted using your User ID. The burden of proving that any Content does not violate any laws or third party rights rests solely with you.

6. INAPPROPRIATE CONTENT. You shall not make the following types of Content available. You agree not to upload, download, display, perform, transmit, or otherwise distribute any Content that (a) is libelous, defamatory, obscene, pornographic, abusive, or threatening; (b) advocates or encourages conduct that could constitute a criminal offense, give rise to civil liability, or otherwise violate any applicable local, state, national, or foreign law or regulation; or (c) advertises or otherwise solicits funds or is a solicitation for goods or services. Company reserves the right to terminate your receipt, transmission, or other distribution of any such material using the Service, and, if applicable, to delete any such material from its servers. Company intends to cooperate fully with any law enforcement officials or agencies in the investigation of any violation of these Terms of Use or of any applicable laws.

Comment: If the website or the service contains communication services such as e-mail, personal web pages, calendars, bulletin board services, chat areas, news, or other communication facilities, consider providing additional restrictions on use of such services, including bans or restrictions on surveys, contests, pyramid schemes, chain letters, junk mail, spam, or unsolicited messages; use of information provided by Company, upload of viruses, Trojan horses, worms, time bombs, cancelbots, corrupted files, or similar software; use of metatag searches of the website or the service; or creating a false identity for the purpose of misleading others. Additionally, qualifications may be added for specific services provided by the company or its affiliates regarding stock quotes, e-mail alerts, online trading, and other services. Consider adding language restricting storage space, length of retention of information in e-mail and other accounts, and the maximum number or size of messages that may be sent from a single account, and providing for termination of an account for inactivity.

7. COPYRIGHT INFRINGEMENT. Company has in place certain legally mandated procedures regarding allegations of copyright infringement occurring on the Site or with the Service. Company has adopted a policy that provides for the immediate suspension and/or termination of any Site or Service user who is found to have infringed on the rights of Company or of a third party, or otherwise violated any intellectual property laws or regulations. Company's policy is to investigate any allegations of copyright infringement brought to its attention. If you have evidence, know, or have a good faith belief that your rights or the rights of a third party have been violated and you want Company to delete, edit, or disable the material in question, you must provide Company with all of the following information: (a) a physical or electronic signature of a person authorized to act on behalf of the owner of the exclusive right that is allegedly infringed; (b) identification of the copyrighted

work claimed to have been infringed, or, if multiple copyrighted works are covered by a single notification, a representative list of such works; (c) identification of the material that is claimed to be infringed or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit Company to locate the material; (d) information reasonably sufficient to permit Company to contact you, such as an address, telephone number, and if available, an electronic mail address at which you may be contacted; (e) a statement that you have a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law; and (f) a statement that the information in the notification is accurate, and under penalty of perjury, that you are authorized to act on behalf of the owner of an exclusive right that is allegedly infringed. For this notification to be effective, you must provide it to Company's designated agent at:

_ _[*Name, Title*]_ _
_ _[*Company Name*]_ _
_ _[*Address*]_ _
_ _[*Phone*]_ _
_ _[*Facsimile*]_ _
_ _[*E-mail*]_ _

8. ALLEGED VIOLATIONS. Company reserves the right to terminate your use of the Service and/or the Site. To ensure that Company provides a high quality experience for you and for other users of the Site and the Service, you agree that Company or its representatives may access your account and records on a case-by-case basis to investigate complaints or allegations of abuse, infringement of third party rights, or other unauthorized uses of the Site or the Service. Company does not intend to disclose the existence or occurrence of such an investigation unless required by law, but Company reserves the right to terminate your account or your access to the Site immediately, with or without notice to you, and without liability to you, if Company believes that you have violated any of the Terms of Use, furnished Company with false or misleading information, or interfered with use of the Site or the Service by others.

9. NO WARRANTIES. *COMPANY HEREBY DISCLAIMS ALL WARRANTIES.* COMPANY IS MAKING THE SITE AVAILABLE "AS IS" WITHOUT WARRANTY OF ANY KIND. YOU ASSUME THE RISK OF ANY AND ALL DAMAGE OR LOSS FROM USE OF, OR INABILITY TO USE, THE SITE OR THE SERVICE. TO THE MAXIMUM EXTENT PERMITTED BY LAW, COMPANY EXPRESSLY DISCLAIMS ANY AND ALL WARRANTIES, EXPRESS OR IMPLIED, REGARDING THE SITE, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. COMPANY DOES NOT WARRANT THAT THE SITE OR THE SERVICE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SITE OR THE SERVICE WILL BE UNINTERRUPTED OR ERROR-FREE.

10. LIMITED LIABILITY. *COMPANY'S LIABILITY TO YOU IS LIMITED.* TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT SHALL COMPANY BE LIABLE FOR DAMAGES OF ANY KIND (INCLUDING, BUT NOT LIMITED TO, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, LOST PROFITS, OR LOST DATA, REGARDLESS OF THE FORESEEABILITY OF THOSE DAMAGES) ARISING OUT OF OR IN CONNECTION WITH YOUR USE OF THE SITE OR ANY OTHER MATERIALS OR SERVICES PROVIDED TO YOU BY COMPANY. This limitation shall apply regardless of whether the damages arise out of breach of contract, tort, or any other legal theory or form of action.

11. AFFILIATED SITES. Company has no control over, and no liability for any third party websites or materials. Company works with a number of partners and affiliates whose Internet sites may be linked with the Site. Because neither Company nor the Site has control over the content and performance of these partner and affiliate sites, Company makes no guarantees about the accuracy, currency, content, or quality of the information provided by such sites, and Company assumes no responsibility for unintended, objectionable, inaccurate, misleading, or unlawful content that may reside on those sites. Similarly, from time to time in connection with your use of the Site, you may have access to content items (including, but not limited to, websites) that are owned by third parties. You acknowledge and agree that Company makes no guarantees about, and assumes no responsibility for, the accuracy, currency, content, or quality of this third party content, and that, unless expressly provided otherwise, these Terms of Use shall govern your use of any and all third party content.

12. PROHIBITED USES. Company imposes certain restrictions on your permissible use of the Site and the Service. You are prohibited from violating or attempting to violate any security features of the Site or Service, including, without limitation, (a) accessing content or data not intended for you, or logging onto a server or

account that you are not authorized to access; (b) attempting to probe, scan, or test the vulnerability of the Service, the Site, or any associated system or network, or to breach security or authentication measures without proper authorization; (c) interfering or attempting to interfere with service to any user, host, or network, including, without limitation, by means of submitting a virus to the Site or Service, overloading, "flooding," "spamming," "mail bombing," or "crashing;" (d) using the Site or Service to send unsolicited e-mail, including, without limitation, promotions, or advertisements for products or services; (e) forging any TCP/IP packet header or any part of the header information in any e-mail or in any posting using the Service; or (f) attempting to modify, reverse-engineer, decompile, disassemble, or otherwise reduce or attempt to reduce to a human-perceivable form any of the source code used by Company in providing the Site or Service. Any violation of system or network security may subject you to civil and/or criminal liability.

13. INDEMNITY. You agree to indemnify Company for certain of your acts and omissions. You agree to indemnify, defend, and hold harmless Company, its affiliates, officers, directors, employees, consultants, agents, and representatives from any and all third party claims, losses, liability, damages, and/or costs (including reasonable attorney fees and costs) arising from your access to or use of the Site, your violation of these Terms of Use, or your infringement, or infringement by any other user of your account, of any intellectual property or other right of any person or entity. Company will notify you promptly of any such claim, loss, liability, or demand, and will provide you with reasonable assistance, at your expense, in defending any such claim, loss, liability, damage, or cost.

14. COPYRIGHT. All contents of Site or Service are: Copyright © 2003 Company, _ _[*company address*]_ _. All rights reserved.

Comment: Consider also listing company and affiliate trademarks displayed on the website or accessed through the service and restricting the use of those trademarks.

15. GOVERNING LAW. These Terms of Use shall be construed in accordance with and governed by the laws of the United States and the State of California, without reference to their rules regarding conflicts of law. You hereby irrevocably consent to the exclusive jurisdiction of the state or federal courts in _ _[*city or county, California, USA*]_ _ in all disputes arising out of or related to the use of the Site or Service.

16. SEVERABILITY; WAIVER. If, for whatever reason, a court of competent jurisdiction finds any term or condition in these Terms of Use to be unenforceable, all other terms and conditions will remain unaffected and in full force and effect. No waiver of any breach of any provision of these Terms of Use shall constitute a waiver of any prior, concurrent, or subsequent breach of the same or any other provisions hereof, and no waiver shall be effective unless made in writing and signed by an authorized representative of the waiving party.

17. NO LICENSE. Nothing contained on the Site should be understood as granting you a license to use any of the trademarks, service marks, or logos owned by Company or by any third party.

18. CALIFORNIA USE ONLY. The Site is controlled and operated by Company from its offices in the State of California. Company makes no representation that any of the materials or the services to which you have been given access are available or appropriate for use in other locations. Your use of or access to the Site should not be construed as Company's purposefully availing itself of the benefits or privilege of doing business in any state or jurisdiction other than California.

Comment: Consider expanding on this provision by expressly stating the intended audience and use of the site, such as promotion of products in the United States, or restricting the use of site, system, or networks by individuals in specified foreign jurisdictions. If jurisdictional issues are anticipated to be problematic, consider making this clause more prominent.

19. MODIFICATIONS. Company may, in its sole discretion and without prior notice, (a) revise these Terms of Use; (b) modify the Site and/or the Service; and (c) discontinue the Site and/or Service at any time. Company shall post any revision to these Terms of Use to the Site, and the revision shall be effective immediately on such posting. You agree to review these Terms of Use and other online policies posted on the Site periodically to be aware of any revisions. You agree that, by continuing to use or access the Site following notice of any revision, you shall abide by any such revision.

Comment: Consider including an integration clause providing that the agreement constitutes the entire agreement

between the parties. Include a reference to any licensing agreements or other agreements incorporated in the terms of use, and an order of priority in the event of any conflict, where necessary.

20. ACKNOWLEDGEMENT. BY USING THE SERVICE OR ACCESSING THE SITE, YOU ACKNOWLEDGE THAT YOU HAVE READ THESE TERMS OF USE AND AGREE TO BE BOUND BY THEM.

Comment: If users access the company's services through a login screen, the terms of use can be set up on a click-through window, preferably with a button for acceptance at the bottom of the window so that users must scroll through the entire terms of use before clicking the button to accept.

© The Regents of the University of California

III. ONLINE SOFTWARE LICENSE AGREEMENTS

§8.4 A. Introduction

With the advent of high speed connections and greater bandwidth for Internet access, software is increasingly being distributed online through electronic downloads. Accordingly, software vendors are digitizing their end-user license agreements and reformatting them for online use. But why impose license agreement terms on online customers? Most vendors wish to address specific contracting terms in a license agreement with their end users, such as:

- The fee, if any, for the license;
- Warranty provisions;
- Disclaimer of implied warranties;
- Limitation of direct damages to the purchase price for the product sold online;
- Exclusion of indirect or consequential damages (such as lost profits);
- Choice of law, choice of forum, or selection of alternate form of dispute resolution;
- Limitation of the licensee's use and scope of use (such as use only for internal purposes or, in the case of freeware or shareware, a prohibition on commercial use or resale);
- Prohibition on decompilation and reverse engineering; and
- Protection of trade secret information through a confidentiality provision.

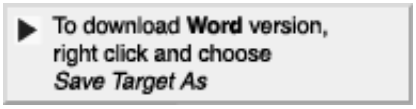
Sections 8.5-8.12 provide sample forms of agreements for use in several types of online licensing situations. The form in §8.5 is a generic end-user software license agreement to accompany the download of a software program. Section 8.6 provides a "beta tester" agreement to be used before the launch of a new software program with third parties who agree to test the software and report back on issues or problems they have encountered in the version they received. The form in §8.9 is an "open source" license for "freeware" distributed by a vendor to educate or otherwise enable the software development community on condition that it not be resold. Section 8.10 contains an evaluation license for a prospective purchaser to try a limited version of software code before actual purchase. The form in §8.12 is a software license for tools to be provided to developers who are integrating drivers or other code from a vendor into their products to maximize interoperability.

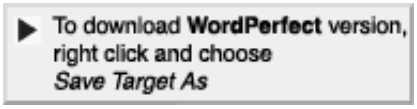
PRACTICE TIP: See §7.13 for some practical suggestions on how to structure an online license agreement to maximize enforceability of its terms. See chap 12 for a review of basic software license terms and a long-form software license agreement with alternative clauses.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/8 Terms of Use; Online Agreements; Linking; Downloading/§8.5 B. Form: Online End-User Software License Agreement

§8.5 B. Form: Online End-User Software License Agreement





ONLINE END-USER SOFTWARE LICENSE AGREEMENT

IMPORTANT! The _ _[*identify/describe software*]_ _ software (the "Software") you seek to download from the _ _[*vendor's name*]_ _ website is licensed only on the condition that you agree to the terms and conditions set forth below. PLEASE READ THE TERMS OF THIS SOFTWARE LICENSE AGREEMENT CAREFULLY.

IF YOU AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT, PLEASE CLICK ON THE BOX ON THIS PAGE LABELED "I ACCEPT," AT WHICH TIME THE SOFTWARE WILL BE DOWNLOADED TO YOUR COMPUTER.

IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PLEASE CLICK ON THE BOX ON THIS PAGE LABELED "I DO NOT ACCEPT," WHICH WILL RETURN YOU TO THE PREVIOUS WEB PAGE WITHOUT DOWNLOADING THE SOFTWARE.

The Software that you are about to access was developed by _ _[*name of vendor*]_ _, a _ _[*state of incorporation*]_ _ corporation ("Vendor") to _ _[*state purpose of software, e.g., help companies manage their inbound and outbound freight shipping processes*]_ _. This End-User License Agreement (this "Agreement") sets forth the terms under which you, as an individual or entity authorized by Vendor (or, for entities, any employee you authorize to use the Software) ("you"), may use the Software.

Comment: If the vendor wants to retain control over who has access to the software when it is being hosted and run remotely, consider including the following provision:

Access to and use of the Software is by permission of Vendor only, and only for applicants who accept this Agreement. Vendor may grant or withhold approval in its sole discretion. If Vendor approves you for use of the Software, Vendor will issue a user identification (the "User ID") and a password (the "Password") that will authorize your access to the Software for the term of this Agreement.

Based on the foregoing and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, you and Vendor agree as follows:

1. NATURE OF AGREEMENT. This Agreement is a legal contract made between you and Vendor. This Agreement contains the terms and conditions that you must comply with if you wish to access and use the Software.

2. LICENSE GRANT. Vendor hereby grants to you a nonexclusive, nonassignable, nonsublicensable license, for your internal use only, for the term of this Agreement, to access and use the Software and any user's guides, specifications, and other related documentation available online (the "Documentation"), subject to the terms and conditions of this Agreement. The licenses granted herein are conditioned upon payment in full for the Software in advance of your download or receipt of the Software.

Comment: Note that this agreement does not include terms regarding payment of the purchase price for the software. The process for purchasing downloadable software can vary, but typically, companies walk the user through several steps, as follows: First, the user selects the desired software by placing it in a "shopping cart;" then the user enters shipping, billing, and credit card information, with the actual purchase conditional on the user's acceptance of the end-user license terms. These terms will appear on the screen along with "I Accept" and "I Do Not Accept" buttons. Once the license is accepted, the purchase can be completed and the download commenced.

3. OWNERSHIP OF SOFTWARE. Vendor retains all rights to the Software and the Documentation not

specifically granted in this Agreement. Vendor owns the Software and the Documentation and all copyright and other intellectual property rights therein, and this Agreement does not transfer to you any title to or any proprietary or intellectual property rights in or to the Software, any updates or derivative works thereto, or the Documentation, or any copyrights, patent rights, or trademarks embodied or used in connection therewith, except for the rights expressly granted in this Agreement. The Software and the Documentation are protected by United States laws and international treaty provisions.

YOU MAY NOT USE, COPY, OR MODIFY THE SOFTWARE, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED FOR IN THIS AGREEMENT.

4. RESTRICTIONS. To the maximum extent permitted by law, you shall not (a) modify, reverse engineer, decompile, disassemble, or attempt to derive the source code of the Software; (b) rent, lease, loan, sell, sublicense, distribute, transmit, or otherwise transfer the Software access to any third party; (c) make any copy of or otherwise reproduce the Software (or any of the browser screens comprising the Software user interface) except for those copies necessarily made by the personal computer and Internet browser that are running the Software; or (4) use the Software to provide service bureau or time-sharing services.

Comment: If the vendor is providing passworded access to the software (see Comment above), then consider adding the following clause at the end of Section 4: "**or (5) disclose your User ID or Password to any third party**." Also consider adding the following:

> **You agree to take all reasonable steps to safeguard your User ID and Password for the Software so as to ensure that no unauthorized person will have access to it, and that no persons authorized to have access will make any unauthorized use. You shall promptly report to Vendor any unauthorized use of the Software of which you become aware and shall take such further steps as may reasonably be requested by Vendor to prevent unauthorized use thereof.**

5. YOUR OBLIGATIONS. You shall be solely responsible for the following: (a) providing all hardware, software, and communications capabilities required for use of the Software, including, without limitation, personal computers with Pentium _ _[*specify minimum CPU speed, e.g., III*]_ _ processors or higher that contain at least _ _[*number, e.g., 64*]_ _ MB of RAM and _ _[*number, e.g., 50*]_ _ MB of available hard disk space, and are equipped with Internet access and a Java-enabled browser such as Netscape Navigator _ _[*specify minimum level, e.g., 4.06*]_ _ or higher; (b) generating, providing, and loading your data into the Software, including, without limitation, freight rates and historical freight data to permit you to use the Software; and (c) providing and maintaining, at all times during the term of this Agreement, the Internet access necessary for your use of the Software.

6. TERM AND TERMINATION. The license granted in this Agreement is effective until terminated. The term of this Agreement and the license grant herein shall commence on the date you agree to this Agreement and download the Software. You may terminate the license and this Agreement at any time on 30 days' prior written notice to Vendor. Vendor may terminate the license and this Agreement at any time on written notice to you that you or your agent has failed to pay any amount due to Vendor under this Agreement. This license shall also terminate automatically on your failure to comply with any of the other terms of this Agreement. On termination of this Agreement, you agree to promptly destroy all printed copies and delete all electronic copies of any documentation that you have downloaded, printed, or created relating to the Software, and to ensure that no copies of any of the Software screens, data, or other content remain archived or otherwise stored on your computers. Notwithstanding termination, the provisions of Sections 3, 6, 7, 8, 9, and 10 of this Agreement shall survive and continue to apply.

7. CONFIDENTIALITY. You agree that you shall not disclose to any third party the Software or any portion thereof, any technical, product, or business information, or any information that Vendor identifies as confidential (collectively, "Confidential Information") related to the Software without the prior written consent of Vendor. You shall maintain the confidentiality of all Confidential Information and shall not use it for any purpose other than the performance of this Agreement.

Notwithstanding the foregoing, Confidential Information does not include information that you can demonstrate was (a) publicly available at the time of disclosure, or later became publicly available through no act or omission by you; (b) in your possession before disclosure by Vendor; or (c) disclosed to you by a third party not in violation of any obligations of confidentiality to Vendor or to any third party.

8. LIMITATION OF LIABILITY. You are not entitled to receive damages from Vendor for any cause relating to

this Agreement, to your use of the Software, to any services provided by Vendor under this Agreement, or to any services provided by any third party in connection with your use of the Software. In addition, in no event shall you be entitled to obtain any injunctive relief or otherwise enjoin, restrain, or otherwise interfere with Vendor or with the distribution, operation, development, or performance of the Software or any related products.

IN NO EVENT SHALL VENDOR BE LIABLE TO YOU FOR ANY DAMAGES WHATSOEVER ARISING OUT OF YOUR USE OF, OR INABILITY TO USE, THE SOFTWARE. IN NO EVENT SHALL VENDOR BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF DATA, LOST PROFITS, OR LOST BUSINESS OPPORTUNITIES, REGARDLESS OF THE LEGAL THEORY UNDER WHICH SUCH DAMAGES ARE SOUGHT, AND EVEN IF ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES. AS SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

9. LIMITED WARRANTY AND DISCLAIMER. Vendor hereby represents and warrants that the Software will, at the time you purchase the Software and for a period of 60 days thereafter, substantially conform to the Documentation in effect on the date of purchase of the Software when given normal, proper, and intended usage in compliance with Vendor's instructions. In the event of a nonconformance during such period, you agree to promptly report such nonconformance along with all information required by Vendor. Vendor shall investigate any such reported nonconformance and shall use commercially reasonable efforts to remedy such nonconformance. If Vendor is unable to remedy such nonconformance within 90 days after the date Vendor has received all relevant information with respect to such nonconformance from you, your sole remedy under this Agreement is to return the Software, delete all copies and all Documentation from your systems, and receive a refund of the price you paid.

TO THE MAXIMUM EXTENT PERMITTED BY LAW, VENDOR EXPRESSLY DISCLAIMS ANY AND ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AS WELL AS ANY WARRANTIES ALLEGED TO HAVE ARISEN FROM CUSTOM, USAGE, OR THE COURSE OF DEALING BETWEEN THE PARTIES. VENDOR DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. IN ADDITION, VENDOR DOES NOT WARRANT OR GUARANTEE THAT YOU WILL BE ABLE TO ACCESS THE SOFTWARE AT ALL TIMES. YOU UNDERSTAND AND ACKNOWLEDGE THAT INTERNET CONGESTION AND OUTAGES, AS WELL AS MAINTENANCE, DOWNTIME, AND OTHER INTERRUPTIONS, MAY INTERFERE AT TIMES WITH YOUR ABILITY TO ACCESS THE SOFTWARE.

10. GOVERNING LAW. This Agreement shall in all respects be governed by and be construed in accordance with the laws of the State of California, without regard to its conflict of laws provisions.

11. FORCE MAJEURE. If the performance of Vendor under this Agreement is prevented, hindered, or otherwise made impractical by reason of flood, strike, war, acts of government, or any other casualty or cause beyond the control of Vendor, then Vendor shall be excused from its performance to the extent and so long as it is prevented, hindered, or delayed by such event(s).

12. SEVERABILITY. If any one or more of the provisions contained in this Agreement shall, for any reason, be held to be invalid, illegal, or unenforceable in any respect, then to the maximum extent permitted by law, such invalidity, illegality, or unenforceability shall not affect any other provision of this Agreement.

13. NO ASSIGNMENT. You may not assign this Agreement or any of the rights granted by Vendor hereunder, in whole or in part, without the prior written consent of Vendor, and any attempt to do so shall be void. This Agreement is binding on and shall inure to the benefit of the parties and their respective successors and permitted assigns.

14. EXPORT CONTROL. You agree to obey and comply with any and all applicable United States laws, rules, and regulations governing the export of software.

15. ACKNOWLEDGEMENT AND EXCLUSIVITY. YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT, AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. YOU FURTHER AGREE THAT IT IS THE COMPLETE AND EXCLUSIVE STATEMENT OF THE AGREEMENT BETWEEN

YOU AND VENDOR, AND THAT IT SUPERSEDES ANY PROPOSAL, PRIOR AGREEMENT, OR UNDERSTANDING, ORAL OR WRITTEN, AND ANY OTHER COMMUNICATION BETWEEN YOU AND VENDOR RELATING TO THE SUBJECT MATTER OF THIS AGREEMENT. THIS AGREEMENT MAY NOT BE CHANGED, ALTERED, OR MODIFIED EXCEPT BY A WRITING SIGNED BY THE PARTIES.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/8 Terms of Use; Online Agreements; Linking; Downloading/ C. Online Beta User Evaluation Agreement/§8.6 1. Introduction

C. Online Beta User Evaluation Agreement

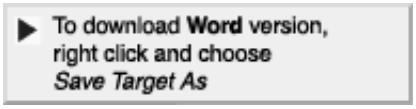
§8.6 1. Introduction

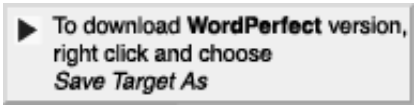
The license agreement in §8.7 is entered into on a royalty-free basis before the launch of a software program with individuals who agree to test the program and report any problems they may find during their use of the program.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/8 Terms of Use; Online Agreements; Linking; Downloading/§8.7 2. Form: Online Beta User Evaluation Agreement

§8.7 2. Form: Online Beta User Evaluation Agreement





ONLINE BETA USER EVALUATION AGREEMENT

IMPORTANT! The _ _[*identify/describe software*]_ _ software (the "Software") you seek to download from the _ _[*vendor's name*]_ _ Website is licensed only on the condition that you agree to the terms and conditions set forth below. PLEASE READ THE TERMS OF THIS SOFTWARE LICENSE AGREEMENT CAREFULLY.

IF YOU AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT, PLEASE CLICK ON THE BOX ON THIS PAGE LABELED "I ACCEPT," AT WHICH TIME THE SOFTWARE WILL BE DOWNLOADED TO YOUR COMPUTER.

IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PLEASE CLICK ON THE BOX ON THIS PAGE LABELED "I DO NOT ACCEPT," WHICH WILL RETURN YOU TO THE PREVIOUS WEB PAGE WITHOUT DOWNLOADING THE SOFTWARE.

This Beta User Evaluation Agreement ("Agreement") sets forth the terms under which you may use the Software for a limited, 30-day evaluation period (the "Evaluation Period"). Evaluation of the Software is by permission of _ _[*vendor's name*]_ _ ("Vendor") only, and only for applicants who accept this Agreement, submit a User Evaluation Request ("Request"), and receive Vendor's approval. Vendor may grant or withhold approval in its sole discretion. If Vendor approves your Request, Vendor will issue a user identification (the "User ID") and a password (the "Password") that will authorize access to the Software for the Evaluation Period.

Based on the foregoing and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, you and Vendor agree as follows:

1. LICENSE GRANT. Vendor hereby grants to you a limited, nonexclusive, nonassignable, nonsublicensable license, for the Evaluation Period only, to access and use the Software and any related documentation available online, subject to the terms and conditions of this Agreement. Unless earlier terminated as provided below, this license shall terminate automatically on expiration of the Evaluation Period, and you will receive no further access to the Software unless and until you have agreed to purchase access to the Software from Vendor under Vendor's standard license agreement.

2. OWNERSHIP. Vendor owns the Software and all copyright and other intellectual property rights in the Software. This Agreement transfers to you neither title to nor any proprietary or intellectual property rights in or to the Software, or any updates or derivative works thereto, or any copyrights, patent rights, or trademarks embodied or used in connection therewith, except for the rights expressly granted in this Agreement. The Software is protected by United States laws and international treaty provisions.

3. RESTRICTIONS. To the maximum extent permitted by law, you may not (a) modify, reverse engineer, decompile, or disassemble the Software; (b) rent, lease, loan, sell, sublicense, distribute, transmit, or otherwise transfer the Software access to any third party; (c) make any copy of or otherwise reproduce the Software (or any of the browser screens comprising the Software user interface) except for those copies necessarily made by the personal computer and Internet browser that are running the Software; (d) disclose your User ID or Password to any third party; or (e) use the Software to provide service bureau or time-sharing services.

You agree to take all reasonable steps to safeguard your User ID and Password for the Software so as to ensure that no unauthorized person will have access to it, and that no persons authorized to have access will make any unauthorized use. You shall promptly report to Vendor any unauthorized use of the Software of which you become aware and shall take such further steps as may reasonably be requested by Vendor to prevent unauthorized use thereof.

4. YOUR OBLIGATIONS. You shall be solely responsible for the following: (a) providing all hardware, software, and communications capabilities required for use of the Software, including, without limitation, personal computers with Pentium _ _[*specify minimum CPU speed, e.g., III*]_ _ processors or higher that contain at least _ _[*number, e.g., 64*]_ _ MB of RAM and _ _[*number, e.g., 50*]_ _ MB of available hard disk space and are equipped with Internet access and a Java-enabled browser such as Netscape Navigator _ _[*specify minimum level, e.g., 4.06*]_ _ or higher; (b) generating, providing, and loading sample freight rates and historical freight data to permit you to evaluate the Software; and (c) providing and maintaining, at all times during the Evaluation Period, the Internet access necessary for your use of the Software.

You agree to use and test the Software during the Evaluation Period. During such testing, you agree to report in writing to Vendor in reasonable detail (a) all occurrences of errors, faults, and problems encountered (including the procedures and tests used to discover and diagnose such errors, faults, or problems) during the operation of the Software, and (b) your observations on the operation of the Software, its functionality, performance, deficiencies, and limitations, together with your recommendations for enhancements to and modifications of the Software. You agree to provide such reports to Vendor from time to time during the term of this Agreement, but no less frequently than monthly.

You understand that the purpose of this Agreement is to solicit your input and comments on the Software and any input or comments you provide are the property of Vendor. You agree that any material, data, information, images, sounds, text, and other communications you transmit or post to a Vendor website or provide to Vendor shall be not be considered confidential ("Communications"). Vendor and its designees shall be free to copy, modify, create derivative works, publicly display, disclose, distribute, license and sublicense through multiple tiers of distribution and licensees, incorporate, and otherwise use the Communications, including derivatives thereof, for any and all commercial or noncommercial purposes without obligation to you of any kind. You hereby assign, and agree to assign, all Communications to Vendor.

5. TERM AND TERMINATION. The term of this Agreement and the license grant herein shall commence on Vendor's approval of your Request and transmission to you of your User ID and Password. Immediately on expiration of the Evaluation Period, this license shall automatically terminate, your User ID and Password will expire, and you will no longer be able to access the Software. This license shall also terminate automatically on your failure to comply with any of the terms of this Agreement. On termination of this Agreement, you agree to promptly destroy all printed copies and delete all electronic copies of any documentation that you have downloaded, printed, or created relating to the Software.

6. CONFIDENTIALITY. You agree that you will not disclose to any third party the Software or any portion thereof, any technical, product, or business information, or any information that Vendor identifies as confidential (collectively, "Confidential Information") related to the Software without the prior written consent of Vendor. You shall take all reasonable measures to maintain the confidentiality of all Confidential Information in your possession or control, which in no event shall be less than the measures that you employ to maintain the confidentiality of your own information of similar importance.

Notwithstanding the foregoing, Confidential Information does not include information that you can demonstrate was (a) publicly available at the time of disclosure, or later became publicly available through no act or omission by you; (b) in your possession before disclosure by Vendor; or (c) disclosed to you by a third party not in violation of any obligations of confidentiality to Vendor or to any third party.

7. LIMITATION OF LIABILITY. You are not entitled to receive damages from Vendor for any cause relating to this Agreement, to your use of the Software, to any services provided by Vendor under this Agreement, or to any services provided by any third party in connection with your use of the Software. In addition, in no event shall you be entitled to obtain any injunctive relief or otherwise enjoin, restrain, or otherwise interfere with Vendor or with the distribution, operation, development, or performance of the Software or any related products.

IN NO EVENT SHALL VENDOR BE LIABLE TO YOU FOR ANY DAMAGES WHATSOEVER ARISING OUT OF YOUR USE OF, OR INABILITY TO USE, THE SOFTWARE, INCLUDING WITHOUT LIMITATION ANY SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF DATA, LOST PROFITS, OR LOST BUSINESS OPPORTUNITIES, REGARDLESS OF THE LEGAL THEORY UNDER WHICH SUCH DAMAGES ARE SOUGHT, AND EVEN IF ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES.

AS SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

8. DISCLAIMER. THE SOFTWARE IS FURNISHED TO YOU "AS IS" WITHOUT ANY WARRANTY. VENDOR EXPRESSLY DISCLAIMS ALL WARRANTIES ON THE SOFTWARE, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ALL IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AS WELL AS ANY WARRANTIES OF NONINFRINGEMENT AND WARRANTIES ALLEGED TO HAVE ARISEN FROM CUSTOM, USAGE, OR A COURSE OF DEALINGS BETWEEN THE PARTIES. EXCEPT AS EXPRESSLY PROVIDED HEREIN, VENDOR SHALL HAVE NO LIABILITY ARISING OUT OF OR IN ANY WAY RELATED TO YOUR USE OF THE SOFTWARE.

IN ADDITION, VENDOR DOES NOT WARRANT OR GUARANTEE THAT YOU WILL BE ABLE TO ACCESS THE SOFTWARE AT ALL TIMES. YOU UNDERSTAND AND ACKNOWLEDGE THAT INTERNET CONGESTION AND OUTAGES, AS WELL AS MAINTENANCE, DOWNTIME, AND OTHER INTERRUPTIONS AT VENDOR'S PLACE OF BUSINESS, MAY INTERFERE AT TIMES WITH YOUR ABILITY TO ACCESS THE SOFTWARE.

9. GOVERNING LAW. This Agreement shall in all respects be governed by and be construed in accordance with the laws of the State of California, without regard to its conflict of laws provisions.

10. SEVERABILITY. If any one or more of the provisions contained in this Agreement shall, for any reason, be held to be invalid, illegal, or unenforceable in any respect, then to the maximum extent permitted by law, such invalidity, illegality, or unenforceability shall not affect any other provision of this Agreement.

11. NO ASSIGNMENT. You may not assign this Agreement or any of the rights granted by Vendor hereunder, in whole or in part, without the prior written consent of Vendor, and any attempt to do so shall be void. This Agreement is binding on and shall inure to the benefit of the parties and their respective successors and permitted assigns.

12. EXPORT CONTROL. You agree to obey and comply with any and all applicable United States laws, rules, and regulations governing the export of software.

13. ARBITRATION. All disputes arising out of or relating to this Agreement shall be finally settled by arbitration conducted in _ _[*city*]_ _, California, under the rules of commercial arbitration of the American Arbitration Association (the "Rules"). Both parties shall bear equally the cost of arbitration (exclusive of legal fees and expenses, all of which each party shall bear separately). All decisions of the arbitrator shall be final and binding on both parties and enforceable in any court of competent jurisdiction. Notwithstanding the foregoing, if a party breaches its obligations under this paragraph, the nonbreaching party may seek injunctive or other equitable relief in any court of competent jurisdiction.

14. ACKNOWLEDGEMENT AND EXCLUSIVITY. YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT, AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. YOU FURTHER AGREE THAT IT IS THE COMPLETE AND EXCLUSIVE STATEMENT OF THE AGREEMENT BETWEEN YOU AND VENDOR, AND THAT IT SUPERSEDES ANY PROPOSAL, PRIOR AGREEMENT, OR UNDERSTANDING, ORAL OR WRITTEN, AND ANY OTHER COMMUNICATION BETWEEN YOU AND VENDOR RELATING TO THE SUBJECT MATTER OF THIS AGREEMENT. THIS AGREEMENT MAY NOT BE CHANGED, ALTERED, OR MODIFIED EXCEPT BY A WRITING SIGNED BY THE PARTIES.

15. FUTURE LICENSE RIGHT. Upon the release by Vendor of a general release version of the Software, Vendor agrees, in consideration of your performance of this Agreement, to license the general release version of the Software to you, in accordance with Vendor's standard software product licensing terms, at a discount of _ _[*number*]_ _% for all orders placed within _ _[*number*]_ _ days of the general release date.

© The Regents of the University of California

D. Open Source Licensing

§8.8 1. Introduction

Under an "open source" license, a vendor discloses its source code to the public free of charge for access, redistribution, and modification. This mechanism can increase the pace of software development and result in lower cost software solutions, but the price is that the vendor no longer has full proprietary rights to the code. This dilution of ownership is viewed as a disincentive for commercial enterprises to adopt open source strategies. Other disincentives include quality concerns, given the open development environment; potential lack of centralized support for the software; and concerns about the lack of warranties accompanying the code. Often, open source software is not accompanied by traditional software warranties.

Open source arrangements are nonetheless of increasing importance in web application and other software development today. The Open Source Initiative, a nonprofit association serving the open source community, provides on its website a definition of the requirements for "open source" software (see http://opensource.org/osr) and a series of forms of open source license agreements that the organization has approved (see http://www.opensource.org/licenses), including the GNU General Public License distributed by the Free Software Foundation (see http://www.fsf.org/licensing/licenses/gpl.html).

A form of open source license, known as the "New BSD License" is presented in §8.9. "BSD" stands for Berkeley Software Distribution, a Unix-type operating system developed at the University of California, Berkeley, for which the original version of the license was used. The original version of the license was revised for use in other contexts, and the resulting forms, such as the one in §8.9, are more properly referred to as modified BSD or BSD-like licenses. The form in §8.9 is nonviral and has few restrictions compared with other free software licenses such as the GNU General Public License.

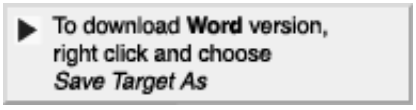
The Federal Circuit has held that open source licenses are enforceable, stating "copyright holders who engage in open source licensing have the right to control the modification and distribution of copyrighted material." *Jacobsen v Katzer* (Fed Cir 2008) 535 F3d 1373, 1381. The *Jacobsen* court granted an injunction to permit an open source developer to enforce the terms of its license, which required the licensee to include certain information in any modified version, such as the original authors' names, the developer's copyright notices, and a description of how the files or computer code had been changed from the original source code. 535 F3d at 1376.

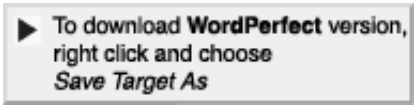
PRACTICE TIP: When presented with open source software, clients should be advised to consider whether the software can be incorporated into products for commercial sale or whether use is restricted to noncommercial purposes. Some licenses that purport to be "open source" include restrictions on use for profit-making purposes. Clients should be advised not to incorporate any such restricted code into products that are intended to be sold commercially.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/8 Terms of Use; Online Agreements; Linking; Downloading/§8.9 2. Form: Open Source Software License Agreement

§8.9 2. Form: Open Source Software License Agreement





Copyright (c), _ _[*Name of copyright owner*]_ _.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

(a) Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.

(b) Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and any other materials provided with the distribution.

(c) Neither the name of the _ _[*organization*]_ _ nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER(S) AND CONTRIBUTOR(S) "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

© The Regents of the University of California

E. Software Evaluation License Agreement

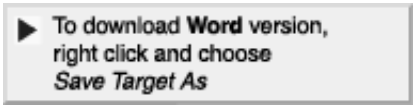
§8.10 1. Introduction

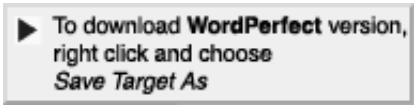
This sample license is an evaluation license for a prospective purchaser to try the software (typically a version with limited functionality or a version with accessibility limited for a specified trial period) on a royalty-free basis before purchasing it, to help the purchaser decide whether to buy the complete version.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/8 Terms of Use; Online Agreements; Linking; Downloading/§8.11 2. Form: Evaluation License Agreement

§8.11 2. Form: Evaluation License Agreement





EVALUATION LICENSE AGREEMENT

IMPORTANT! The Software you seek to download from the _ _[*name of vendor*]_ _ Website is licensed only on the condition that you agree with the terms and conditions set forth below. PLEASE READ THE TERMS OF THIS SOFTWARE LICENSE AGREEMENT CAREFULLY.

IF YOU AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT, PLEASE CLICK ON THE BOX ON THIS PAGE LABELED "I ACCEPT," AT WHICH TIME THE SOFTWARE WILL BE DOWNLOADED TO YOUR COMPUTER.

IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PLEASE CLICK ON THE BOX ON THIS PAGE LABELED "I DO NOT ACCEPT," WHICH WILL RETURN YOU TO THE PREVIOUS WEB PAGE WITHOUT DOWNLOADING THE SOFTWARE.

1. DEFINITIONS

1.1. "Materials" are the _ _[*describe/identify software*]_ _ software, related documentation, license key codes, and other materials, including any updates and upgrade thereto, that are provided to you under this Agreement. Materials also include the Redistributables (defined in Section 1.2).

1.2. "Redistributables" are the files listed in the "redist.txt" file that is included in the Materials. If there is no redist.txt file included in the Materials, then there are no Redistributables.

2. LICENSE GRANT. Subject to all of the terms and conditions of this Agreement, _ _[*name of vendor*]_ _ ("Vendor") grants to you a nonexclusive, nonassignable license to use the Materials for a limited, _ _[*number*]_ _-day evaluation period (the "Evaluation Period"). The license granted herein is royalty-free.

3. LICENSE RESTRICTIONS

3.1. If you receive your first copy of the Materials electronically, and a second copy on media, then you may use the second copy only in accordance with your applicable license stated in this Agreement, or for backup or archival purposes. You shall not make the second copy available to any other user.

3.2. You shall not (a) use or copy the Materials except as provided in this Agreement; (b) rent or lease the Materials to any third party; (c) assign this Agreement or transfer the Materials; (d) modify, adapt, or translate the Materials in whole or in part; (e) reverse engineer, decompile, or disassemble the Materials; (f) attempt to modify or tamper with the normal function of a license manager that regulates usage of the Materials; or (g) distribute, sublicense, or transfer the source code form of any components of the Materials and any derivatives thereof to any third party.

3.3. You as an individual shall use the Materials only for internal evaluation purposes and only for the term of the Evaluation Period. You may install copies of the Materials on an unlimited number of computers provided that you are the only individual using the Materials and only one copy of the Materials is in use at any one time. You shall not distribute any portion of the Materials. A separate license is required for each additional use and/or individual user in all other cases. Vendor shall provide you with a license code key that enables the Materials for an Evaluation license. If you are an entity, Vendor grants you the right to designate one individual within your organization to have the sole right to use the Materials in the manner provided above.

4. COPYRIGHT. Title to the Materials and all copies thereof remain with Vendor or its suppliers. The

Materials are copyrighted and are protected by United States copyright laws and international treaty provisions. You agree not to remove any copyright notice from the Materials. You agree to prevent any unauthorized copying of the Materials. Except as expressly provided herein, Vendor does not grant any express or implied right to you under Vendor patents, copyrights, trademarks, or trade secret information.

5. REPLACEMENTS. The Materials are provided "AS IS" without warranty of any kind. If the media on which the Materials are furnished are found to be defective in material or workmanship under normal use for a period of _ _[*number*]_ _ days from the date of receipt, Vendor's entire liability and your exclusive remedy shall be the replacement of the media. This warranty is void if the media defect results from accident, abuse, or misapplication.

6. LIMITATION OF LIABILITY. THE REPLACEMENT PROVISION IN SECTION 5 IS THE ONLY WARRANTY OF ANY KIND. VENDOR MAKES NO OTHER WARRANTY, EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY, OR FITNESS FOR A PARTICULAR PURPOSE. NEITHER VENDOR NOR ITS SUPPLIERS SHALL BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF, OR THE INABILITY TO USE, THE SOFTWARE, EVEN IF VENDOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

BECAUSE SOME JURISDICTIONS PROHIBIT THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

7. USER SUBMISSIONS. You agree that any material, data, information, images, sounds, text, and other communications you transmit or post to a Vendor website or provide to Vendor ("Communications") shall be not be considered confidential. Vendor and its designees shall be free to copy, modify, create derivative works, publicly display, disclose, distribute, license and sublicense through multiple tiers of distribution and licensees, incorporate, and otherwise use the Communications, including derivatives thereof, for any and all commercial or noncommercial purposes without obligation of any kind to you.

8. TERMINATION. This Agreement becomes effective on the date you accept this Agreement and shall continue until the end of the Evaluation Period, at which time it will automatically terminate. Vendor may terminate this Agreement at any time if you breach any of its terms and conditions. On termination, you shall either immediately destroy the Materials or return all copies of the Materials to Vendor along with any copies you have made.

9. APPLICABLE LAW. Any claim arising under or relating to this Agreement shall be governed by the internal substantive laws of the State of California, without regard to its conflict of laws rules. You shall not export the Materials in violation of applicable export laws.

© The Regents of the University of California

F. Online Software Developer Toolkit License Agreement

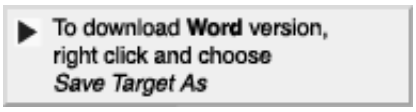
§8.12 1. Introduction

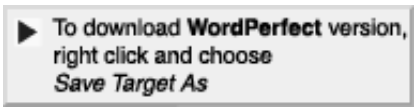
The following form of online software license is intended to be used in connection with tools to be provided to developers who are integrating drivers or other code from a vendor into their own products to maximize interoperability.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/8 Terms of Use; Online Agreements; Linking; Downloading/§8.13 2. Form: Online Software Developer Toolkit License Agreement

§8.13 2. Form: Online Software Developer Toolkit License Agreement





ONLINE SOFTWARE DEVELOPER TOOLKIT LICENSE AGREEMENT

IMPORTANT! The Software you seek to download from the _ _[*name of vendor*]_ _ Website ("Website") is licensed only on the condition that you ("you" or the "Developer") agree with _ _[*name of vendor*]_ _ ("Vendor") to the terms and conditions set forth below. PLEASE READ THE TERMS OF THIS SOFTWARE LICENSE AGREEMENT CAREFULLY.

IF YOU AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT, YOU SHOULD CLICK ON THE BOX ON THIS PAGE LABELED "I ACCEPT," AT WHICH TIME THE SOFTWARE WILL BE DOWNLOADED TO YOUR COMPUTER.

IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, YOU SHOULD CLICK ON THE BOX ON THIS PAGE LABELED "I DO NOT ACCEPT," WHICH WILL RETURN YOU TO THE PREVIOUS WEB PAGE WITHOUT DOWNLOADING THE SOFTWARE.

Vendor grants to Developer a license to use the Software and documentation (the Software and the documentation are referred to herein as "Licensed Materials"), under the following terms and conditions:

1. DEFINITIONS. The following capitalized terms used in this Agreement are defined as follows:

1.1. "Software" means the _ _[*describe/identify the software*]_ _ software downloaded from this Website, which include certain device driver programs (hereinafter referred to as "Driver").

1.2. "Hardware" means any computer system running the _ _[*describe operating system, e.g., Windows 2000 or Windows XP*]_ _ operating system and owned by Developer.

1.3. "Products" means any of the peripheral devices identified in Exhibit A.

Comment: This agreement is intended for a developer who is incorporating software owned by the vendor into a hardware product manufactured by the developer or a third party (*e.g.,* a printer driver that will permit a printer to take instructions from a word processing program or operating system). This agreement requires the developer to identify the hardware products in an exhibit to be completed electronically before the contract is deemed to be accepted by the vendor.

1.4. The Software is "Used" or in "Use" when it is loaded into temporary memory (*i.e.,* RAM) or installed into permanent memory (*i.e.,* hard disk, CD-ROM, or other storage device) of the Hardware.

1.5. "Effective Date" means the date on which the Developer clicks the "I ACCEPT" button on this page and downloads the Software.

2. LICENSE GRANT

2.1. Vendor grants to Developer a nonexclusive, nontransferable license to Use one copy of the Software on the Hardware for development of certain software and the adaptation of the Driver to be used in conjunction with the Products described in Exhibit A.

2.2. Developer may incorporate the Driver in the applications program developed by Developer, may make unlimited copies of the Driver as contained in the applications program, and may distribute, market, and

license the applications program to end users either directly or through traditional channels of distribution.

Comment: Note that two license grants are necessary to cover the two intended uses of the software. First, the developer will need to load the software onto its own computers to do the integration and programming necessary to make the driver work with its peripheral devices. The license grant in Section 2.1 authorizes the developer to use one copy of the software for this purpose. Second, in order to distribute copies of the driver that it develops (which is a derivative work of the original software), the developer will need another license from the vendor to make multiple copies for its own end users, to be loaded into all the products that the developer sells. The license grant in Section 2.2 covers these distribution rights.

2.3. Developer may make one copy the Software for archival purposes. Developer shall have no right to reproduce any documentation downloaded from the Website relating to the Software.

2.4. Developer shall not, and shall not authorize any third party to, (a) reverse engineer, disassemble, create derivative works, and/or modify the Software; (b) rent, lease, sell, transfer, or further sublicense the Software; (c) electronically transfer the Software; (d) translate the Software into another computer language; (e) reproduce or distribute the Software, or the Driver, other than as specifically authorized in this Agreement; or (f) export the Materials in violation of applicable export laws.

3. OWNERSHIP; NOTICE. The Software, and all intellectual property contained therein, are and shall remain the sole and exclusive property of Vendor and its licensors, and are protected by United States copyright laws and international copyright treaty provisions. Developer shall include any proprietary notices embodied in the Software on any copy of the Software in any form, in whole or in part. Any modifications to the Software made by Developer shall be owned by Vendor but are licensed to Developer on the same terms as set forth in this Agreement. Developer hereby assigns and agrees to assign ownership of such modifications to Vendor.

4. MAINTENANCE; SUPPORT

4.1. Vendor shall use commercially reasonable efforts to provide reasonable amounts of technical support at no charge to Developer for the Software used in connection with the Products identified in Exhibit A only. Vendor, however, is under no obligation to provide any specific level or amount of support to Developer.

4.2. Developer may provide Vendor with notice at any time of any defects it claims are contained in the Software. Vendor makes no warranty that a defect brought to its attention will be corrected or that a revision, if made, will cause the Software to operate in any particular manner.

4.3. Vendor shall have no obligation to provide technical support for any claim based on (a) the use of the Software in connection with or in combination with hardware, software, or data not intended for use with the Software; (b) the use of the Software other than as permitted under this Agreement or in a manner for which it was not intended; (c) any modification made to the Software by Developer or any third party; or (d) if Vendor has advised the Developer to cease its Use of the Software.

5. TERM; TERMINATION. This Agreement is effective from the Effective Date and shall continue until the second anniversary of the Effective Date, at which time it shall automatically terminate. This Agreement may be terminated at any time by either party on 30 days' prior notice to the other party. Vendor may terminate this Agreement at any time without notice if Developer fails to comply with any term or condition of this Agreement. On termination, Developer shall permanently delete and destroy the Licensed Materials, together with all copies thereof.

6. LICENSE FEE. The license granted herein is royalty-free.

Comment: Because the vendor desires to encourage developers to include code that makes the developers' products compatible with the vendor's software, granting free rights to the toolkits necessary for this compatibility is a common practice. Software vendors normally do not want to create impediments to broad compatibility.

7. CONFIDENTIALITY

7.1. Developer hereby agrees that it shall keep confidential any information or data obtained from Vendor in connection with this Agreement ("Confidential Information") and shall not divulge the same to any third parties,

except for (a) information that, at the time of disclosure, had been previously made public; (b) information that is made public after disclosure to Developer, unless such disclosure is a breach of this or any other agreement; (c) information that, before disclosure to Developer, was already in Developer's possession without obligation of confidentiality; or (d) information that, subsequent to disclosure, was obtained by Developer from a third party who was lawfully in possession of such information and was not in violation of any obligation of confidentiality to Vendor or any Vendor licensee.

7.2. All Confidential Information shall remain the sole property of Vendor. Developer shall have no implied licenses or other rights in the Confidential Information not specifically granted herein. Developer shall not disclose the Confidential Information to anyone other than its employees and contractors with a demonstrable need to know such information and who have entered into a binding, written, confidentiality obligation to Developer that protects such Confidential Information against unauthorized disclosure or use.

7.3. Developer shall take all reasonable precautions to keep the Confidential Information confidential and to prevent unauthorized use or disclosure of the Confidential Information. Developer acknowledges that any unauthorized use or disclosure of the Confidential Information would cause irreparable harm to Vendor.

7.4. On termination of this Agreement, Developer shall destroy all Confidential Information within 3 days of the date of termination.

7.5. The obligations in this Section 7 shall survive for a period of 3 years from the date of termination of this Agreement.

8. LIMITED WARRANTIES. Vendor warrants to Developer that the Software has the functionality described in the applicable documentation. This warranty shall be limited in duration to 90 days from the Effective Date. Developer's remedy under this provision is set forth in Section 4 above.

Comment: Consider listing the applicable documentation in detail. Further, consider whether, under the circumstances, this warranty and any maintenance obligations on the part of the vendor should be deleted and replaced with an "as is" license. Given that this agreement in intended to encourage developers to work with the vendor's products, it is likely that some degree of support will be necessary for the developers to be willing to proceed.

9. WARRANTY DISCLAIMERS; LIABILITY LIMITATIONS

9.1. EXCEPT AS SPECIFICALLY SET FORTH IN SECTION 8 ABOVE, VENDOR MAKES NO WARRANTY OR REPRESENTATION WITH RESPECT TO THE SOFTWARE AND IT IS LICENSED "AS IS." THE WARRANTY AND REMEDY PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. ANY STATEMENTS OR REPRESENTATIONS MADE BY ANY OTHER PERSON OR ENTITY ARE VOID.

9.2. DEVELOPER ASSUMES ALL RISK AS TO THE SELECTION, USE, PERFORMANCE, AND QUALITY OF THE LICENSED MATERIALS. IN NO EVENT SHALL VENDOR OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION, OR DELIVERY OF THE SOFTWARE BE LIABLE FOR SPECIAL, DIRECT, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF PROFITS OR INABILITY TO USE THE SOFTWARE, EVEN IF VENDOR OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Comment: If a fee is charged for the software materials, consider adding:

> **IN NO EVENT SHALL VENDOR'S LIABILITY FOR ANY DAMAGES OR LOSS TO DEVELOPER OR TO ANY THIRD PARTY IN CONNECTION WITH THIS AGREEMENT EXCEED ANY LICENSE FEE ACTUALLY PAID BY THE DEVELOPER FOR THE LICENSED MATERIALS.**

Comment: Further consider whether it is appropriate to add the following:

> **THE SOFTWARE IS NOT DESIGNED, INTENDED, OR AUTHORIZED FOR USE IN ANY MEDICAL, LIFE-SAVING OR LIFE-SUSTAINING SYSTEMS, OR FOR ANY OTHER APPLICATION IN WHICH THE FAILURE OF THE MATERIALS COULD CREATE A RISK OF PERSONAL INJURY OR DEATH. Should you use the Software for any such unintended or unauthorized use, you shall indemnify and hold Vendor and its officers, subsidiaries, and affiliates harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out**

of, directly or indirectly, any claim of product liability, personal injury, or death associated with such unintended or unauthorized use, even if such claim alleges that Vendor was negligent regarding the design or manufacture of the part.

9.3. Because some states and/or countries do not allow limitations on how long an implied warranty lasts and some states and/or countries do not allow the exclusion or limitation of incidental or consequential damages, the preceding limitation and exclusion may not apply to Developer. This warranty gives Developer specific legal rights, and Developer may also have other rights which vary from state to state and/or country to country.

10. GENERAL PROVISIONS

10.1. If any provision or portion of a provision of this Agreement is determined to be invalid or unenforceable, it shall be deemed omitted and the remaining provisions of this Agreement shall remain in full force and effect.

10.2. This Agreement is governed by and shall be construed in accordance with the internal laws of the State of California, without regard to choice-of-law rules.

10.3. This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof, and all prior agreements, representations, statements, and undertakings are hereby expressly cancelled.

10.4. Neither party hereto shall be liable in any manner for any failure or delay in fulfillment of all or part of this Agreement directly or indirectly caused by any causes or circumstances beyond its reasonable control, including, but not limited to, acts of God.

10.5. Developer may not assign or transfer all or part of this Agreement to any third party without the express written approval of Vendor.

10.6. Any dispute between the parties relating to this Agreement that cannot be resolved through mutual negotiation shall be subject to arbitration in _ _[*city*]_ _, California in accordance with the Commercial Arbitration Rules of the American Arbitration Association. Any such arbitration must be initiated no later than one year from the date the dispute arose.

© The Regents of the University of California

IV. LINKING ARRANGEMENTS

§8.14 A. Introduction

As part of their business model, many website operators wish to provide users with access to information on other websites. As the Internet has expanded, users increasingly depend on search engines and websites that aggregate data from other websites to find their way around. It also becomes tempting for website operators to leverage off of data and functionality created by others to make their own sites more appealing. Search engines, comparison shopping sites, travel sites, and other sites that aggregate data from different sources depend on accessing content on third party websites. So-called "peer-to-peer networks" provide individuals the opportunity to share data and content directly, often without the need to access a central server. Sections 8.15-8.17 and 8.19-8.24 review the legal implications of accessing third party Internet websites and sharing third party content. A sample form of linking agreement is provided in §8.18.

© The Regents of the University of California

B. Linking and Framing

§8.15 1. Generally

A "link" is an embedded instruction to a browser program to point to another location on the Internet—a way of connecting the information on two websites or files or between different points of a single file. Generally, two types of links are used. The first is a "hypertext reference," sometimes known as an "out link." The user typically activates this type of link by clicking on an icon or highlighted text. When activated, the out link will take the user out of the Internet site currently being viewed and onto another site. Here, the link is the means by which the user exits the site currently being viewed. In a variation of this concept, known as "deep linking," the out link to the third party site bypasses the third party site's home page and takes the user directly to specific content within the third party site.

The second kind of link is an "inline link" or an "image link" by which text or images from another web site are imported into the website that the user is currently viewing. See *Kelly v Arriba Soft Corp.* (9th Cir 2003) 336 F3d 811. An inline link is not necessarily perceptible to the user and does not cause the user to exit the site currently being viewed. The third party content may be displayed on the site the user is currently viewing, perhaps combined with text and images from the host site. Sometimes the third party content subject to the inline link is surrounded by a "frame" of content from the host site, which is called "framing."

© The Regents of the University of California

§8.16 2. Copyright Infringement Issues

In *Ticketmaster Corp. v Tickets.com, Inc.* (CD Cal 2000) 54 USPQ2d 1344, the federal district court ruled that hyperlinking alone does not violate the Copyright Act because it does not involve copying. Tickets.com operated an Internet site that sold tickets to events and, when tickets to a particular event were available only through a third party, it directed users out of its site through hypertext outlinks to appropriate third party websites, including Ticketmaster's. Tickets.com used deep links to send users to the page of Ticketmaster's website relating to the specific event of interest, bypassing Ticketmaster's home page.

Ticketmaster sued, claiming copyright infringement among other things. The court ruled that it is not copyright infringement to take basic facts from publicly available web pages and use those facts, provided that the expression and method of presentation is not copied. The court held that:

> [H]yperlinking does not itself involve a violation of the Copyright Act… since no copying is involved, the customer is automatically transferred to the particular genuine web page of the original author. There is no deception in what is happening. This is analogous to using a library's card index to get reference to particular items, albeit faster and more efficiently.

For additional discussion of the *Ticketmaster* litigation, see §18.21.

PRACTICE TIP: Linking also raises trademark issues if the link consists of the linked site's trademark. There may be a danger of confusing website visitors about the source, affiliation, or sponsorship of the linked company's goods or services, and the link may imply an endorsement. See generally §§3.26-3.70.

© The Regents of the University of California

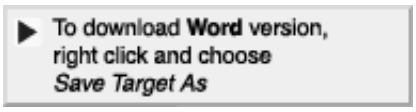
§8.17 3. Potential Liability for Trespass to Chattels

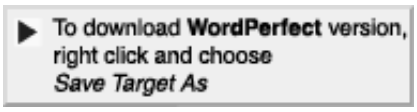
Web sites known as "aggregators" use automated search tools (known as "bots" or "crawlers") to gather information from other sites and create multiple links to that information for the benefit of users. These aggregator sites provide many advantages to users: They save users time by consolidating links to needed data in one place and facilitating comparison shopping. This business model has come under fire. In *eBay, Inc. v Bidder's Edge, Inc.* (ND Cal 2000) 100 F Supp 2d 1058, the court granted a preliminary injunction restricting Bidder's Edge from using "bots" to gather data from eBay's site. Bidder's Edge collected information about online auctions and directed users to the best online price available. The court ruled that the use of automated search programs to collect information from web sites amounted to trespass to chattels. The court found it significant that the use of eBay's systems burdened its computer systems. Permitting Bidder's Edge to engage in this activity could encourage others to do the same and cause eBay "irreparable harm from reduced system performance, system unavailability, or data losses." 100 F Supp 2d at 1066. For further discussion of the tort of trespass to chattels in the context of the Internet, see §§18.17-18.21.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/8 Terms of Use; Online Agreements; Linking; Downloading/§8.18 C. Form: Linking Agreement

§8.18 C. Form: Linking Agreement





LINKING AGREEMENT

_ _[*Name of Company*]_ _ appreciates your interest in placing links to the _ _[*Company's website address*]_ _.com website and _ _[*name of Company*]_ _'s logo on your website. If you would like to place a link on your website, you must do the following:

Read the linking agreement set forth below;

Select "I Agree" below;

Complete the contact information; and

Download the _ _[*name of Company*]_ _.com logo and create the _ _[*Name of Company*]_ _.com link

1. LICENSE

_ _[*Name of Company*]_ _ ("Company") hereby grants to you, and you hereby accept, a nonexclusive, nontransferable license to display a Link (as defined below) to the home page of Company on the website owned or operated by you ("Your Site"). Such Link shall consist solely of the Company logo (the "Logo") as specified by Company from time to time. You may not modify, edit, or alter the Logo in any manner. Nothing in this Agreement shall grant to you any rights in the Logo, the Company site, or any other intellectual property of Company or any of its affiliates, other than as expressly set forth in this Agreement. For purposes of this Agreement, "Link" shall mean a hypertext link located on Your Site which shall link directly to the home page of Company located at www._ _[*Company's domain name*]_ _ (as such URL may be modified from time to time), and which shall be implemented by you solely in accordance with this Agreement.

2. GUIDELINES

You agree to comply with the following guidelines:

2.1. You may use the Logo only in the specific format provided to you by Company, as the Logo and format may be modified and provided to you by Company from time to time. The Logo and format shall be provided to you only after you agree to be bound by the terms and conditions of this Agreement by clicking on the "I Agree" button at the bottom of this page.

2.2. You may use the Logo only on Your Site, and not in any other manner. The Logo must always be an active link to the homepage of the Company site and not to any other page, as "deep linking" past the Company homepage is strictly prohibited. Any Links must display such homepage exactly as it has been created by Company; no "framing" or other alterations or additions are permitted.

2.3. The Logo may be used only on web pages that make accurate references to Company or its products or services, and must be displayed adjacent to the reference or at the bottom of the same page. The Logo should not be the most prominent element on Your Site's web pages. Your web page title and other trademarks and logos must appear at least as prominently as the Logo. You may not display the Logo in any manner that implies sponsorship, endorsement, or license by Company, or in any manner that can be reasonably interpreted to suggest that editorial content on Your Site has been authored by, or represents the view or opinions of, Company.

2.4. The Logo must appear by itself, with a minimum of 10 pixels of spacing between each side of the Logo and the other graphic or textual elements on your page. The Logo may not be used as a feature or design

element of any other logo.

2.5. You may not alter the Logo or any elements thereof in any manner, including size, proportions, colors, etc., nor may you animate, morph, or otherwise distort their perspective or appearance.

2.6. You may not use the Logo on any site that disparages Company or any of its affiliates or their respective personnel, products, or services.

2.7. Company reserves the right to change or discontinue any or all segments of its website without notice.

2.8. Company is not responsible for the content available on any websites linked to the Company website, and access to any such website is at the user's own risk.

3. REPRESENTATIONS AND WARRANTIES. You hereby represent and warrant to Company that (a) you have the right, power, and authority to enter into this Agreement and perform your obligations as set forth herein; (b) you are under no obligation or restriction that does or would interfere or conflict with your obligations under this Agreement, nor shall you assume any such obligation or restriction; and (c) the information provided by you in connection with this Linking Agreement is true, correct, and complete.

4. COVENANTS. You hereby covenant and agree with Company that (a) you shall comply with Company's Privacy Policy and User's Agreement, each as in effect from time to time; (b) Your Site shall not be operated in violation of any applicable federal, state, or local law, rule or regulation; (c) the content included on Your Site, as well as the operation of Your Site, will not violate or infringe the copyright, trademark, trade name, patent, literary, intellectual, artistic, dramatic, publicity, or privacy, or any other right of any entity or person or contain any material that is libelous, slanderous, or obscene; (d) if any of the information provided in this Section 4 changes at any time, you shall notify Company as specified below in Section 10; and (e) Your Site shall not publish, link to, sell, or otherwise distribute Adult Content (as defined below), and you shall remove any such Adult Content as soon as you become aware, or are made aware, of such Adult Content. For purposes of this Agreement, "Adult Content" means any material, including textual, audio, or video material, that is violent or pornographic or that contains nudity, explicit violent or sexual material, or depictions of violent or sexual acts.

5. USE OF DATA. You shall not have the right to use, publish, share, sell, or otherwise distribute any data collected with respect to users of Your Site that relate to (a) their clicking on a Link, (b) their use of _ _[*Company's website*]_ _, or (c) any other information deemed proprietary by Company.

6. DISCLAIMER OF WARRANTIES. COMPANY HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY, WITH RESPECT TO THE LOGO, COMPANY'S WEBSITE, OR OTHERWISE, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF NONINFRINGEMENT, TITLE, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. Company obtains the content appearing on Company's website from sources that it considers to be reliable; however, neither Company nor any of its vendors warrants the accuracy or completeness of such content.

7. LIMITATION OF LIABILITY. IN NO EVENT SHALL COMPANY BE LIABLE FOR ANY DAMAGES OF ANY KIND, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, CONSEQUENTIAL, SPECIAL, INCIDENTAL, OR PUNITIVE DAMAGES, OR FOR ANY LOST PROFITS, SAVINGS, DATA, OR USE, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY (INCLUDING NEGLIGENCE OR STRICT LIABILITY), ARISING OUT OF THIS AGREEMENT. BOTH PARTIES ACKNOWLEDGE AND AGREE THAT NO MONETARY PAYMENT IS REQUIRED UNDER THIS AGREEMENT AND THE LACK OF SUCH PAYMENT IS BASED IN PART ON THESE LIMITATIONS. THE PARTIES FURTHER AGREE THAT THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. Without limiting the foregoing, Company shall have no responsibility for any monetary damages under any contract, tort, or other legal or equitable theory, regardless of the form of the action. Such limit shall apply whether or not Company has been advised of the possibility of such damages.

8. INDEMNITY. You agree to indemnify and hold harmless Company, its affiliates, and their respective officers, directors, employees, and agents from and against any and all claims, actions, suits, or proceedings, as well as any and all losses, liabilities, damages, costs, and expenses (including reasonable attorney fees) arising out of or accruing from (a) any misrepresentation or breach of your representations and warranties set forth in this Agreement; and (b) any noncompliance by you with any covenants, agreements, or undertakings contained in or made under this Agreement.

9. TERM AND TERMINATION

9.1. The term of this Agreement shall begin on the date you agree to be bound by the terms hereof by clicking on the button below labeled "I Agree" and shall continue until terminated as provided herein.

9.2. Company may terminate this Agreement or modify your permission to display the Logo at any time with or without cause in Company's discretion on notice to you.

9.3. You may terminate this Agreement at any time on 30 days' prior written notice to Company.

9.4. This Agreement shall terminate automatically if, at any time, you are in violation of this Agreement.

9.5. Company has the sole right to own and/or control the content displayed on its website, including, but not limited to, all copyrights, trademarks, trade names, service marks, and other proprietary rights. Whether or not Company terminates this Agreement as provided herein, Company reserves the right to take action against any use that does not conform to this Agreement, infringes any intellectual property or other right of Company, or violates applicable law.

9.6. Immediately on the termination of this Agreement, you shall disconnect all links to the Company's website and cease all use of the Logo. The provisions of Sections 3, 4, 5, 6, 7, 8, 9(f), 11, and 13 hereof shall survive the termination of this Agreement.

10. NOTICES. Any notice required or permitted by this Agreement shall be in writing and shall be deemed sufficient on receipt, when delivered personally or by courier, overnight delivery service, confirmed facsimile, or confirmed e-mail, or 48 hours after being deposited in the regular mail as certified or registered mail with postage prepaid. Notices to you shall be sent to the address specified by you in the contact information screen that will appear when you click on "I Agree" below. Notices to Company should be sent to the following address:

_ _[*Name of Company*]_ _
_ _[*Street address*]_ _
_ _[*City, state, and zip*]_ _
_ _[*Fax*]_ _
_ _[*E-mail*]_ _
_ _[*Name of contact person*]_ _
_ _[*Telephone*]_ _

You may change your address for notices by giving us written notice in the manner set forth above. Company may change its address for notices by updating this page. If you have not indicated an address, or if your address is no longer current, Company may use (a) the address indicated for the owner of the URL of Your Site in the database maintained by Network Solutions, Inc., or any other applicable domain registration authority, or (b) the e-mail address of the webmaster of Your Site, or any other similar e-mail address specified on Your Site.

11. GOVERNING LAW; JURISDICTION. This Agreement shall be governed by and construed in accordance with the laws of the State of California, without regard to the conflicts-of-laws provisions thereof. The parties hereby submit to the exclusive jurisdiction of the federal and state courts located in the County of _ _[*name of county*]_ _, and any action or suit under this Agreement shall only be brought by the parties in any federal or state court with appropriate jurisdiction over the subject matter established or settled in the County of _ _[*name of county*]_ _.

12. AMENDMENT. Company reserves the right in its sole discretion to amend this Agreement by providing you with prior written notice thereof. If you do not wish to be bound by any such amendments, you may terminate this agreement within 30 days of receiving notice of such amendment by providing written notice of termination to Company.

13. INTEGRATION. This Agreement constitutes the entire agreement between the parties and supersedes all oral or written agreements and understandings made and entered into by the parties before the date hereof.

14. ASSIGNMENT; BINDING EFFECT. You may not assign this Agreement in whole or in part without the prior written consent of Company, and any purported assignment in violation of this provision shall be null and void. Subject to the foregoing limitation, this Agreement is binding on and shall inure to the benefit of the parties hereto, their respective heirs, personal representatives, successors, and assigns.

15. SEVERABILITY. If any provision of this Agreement is held by a court of competent jurisdiction to be illegal, invalid, or unenforceable, the remaining provisions shall remain in full force and effect.

16. WAIVER. No waiver of any breach of any provision of this Agreement shall constitute a waiver of any prior, concurrent, or subsequent breach of the same or any other provisions hereof, and no waiver shall be effective unless made in writing and signed by an authorized representative of the waiving party.

17. NO OTHER RELATIONSHIP. This Agreement shall not be construed or deemed to create any partnership, joint venture, agency, franchise, or other form of agreement or relationship than as expressly set forth herein.

Date: _ _ _ _ _ _

_ _[*NAME OF COMPANY*]_ _,
a _ _[*state of incorporation*]_ _ **corporation**

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

Date: _ _ _ _ _ _

_ _[*NAME OF OTHER PARTY*]_ _,
a _ _[*state of incorporation*]_ _ **corporation**

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

Comment: This agreement contemplates a "free" linking arrangement for informational purposes only. Parties often create cross-linking, cross-promotional arrangements that result in payments based on various metrics such as "click-throughs" (the number of users who click the link and enter the target site) or measures of the value that the click-through provided to the target site in terms of length of stay on the site, number of pages viewed, or transactions completed.

© The Regents of the University of California

V. DOWNLOADING AND UPLOADING CONTENT

§8.19 A. Generally

Many Internet business models involve the downloading or uploading of images, text, or other content. Downloading means the process of transferring data from a website to a user's computer system. Uploading is transmission in the other direction, from the user's computer system to the server on which the web site is operated. People who share images or other content with others on bulletin board systems upload files from their computers to the bulletin board service on the Internet. Other users can then browse through this content and download files of interest to them.

The File Transfer Protocol (FTP) is the Internet protocol for downloading and uploading files. If downloading and uploading occur through a web page, the FTP request is set up and operated by functionality embedded in the web page. The user normally receives an automatically generated request for a destination on the user's hard disk for the downloaded file. Once this destination is confirmed, the download transmission takes place.

© The Regents of the University of California

§8.20 B. Copyright Infringement Issues

Downloading and uploading content have been held to constitute copyright infringement. In cases involving bulletin board sites (BBS) in which end users copy and upload infringing materials, courts have analyzed the infringement liability of a BBS with reference to the copyright holder's reproduction rights, public display rights, and public distribution rights. See, *e.g., Marobie-Fl, Inc. v National Ass'n of Fire Equip. Distribs.* (ND Ill 1997) 983 F Supp 1167; *Sega Enters. Ltd. v MAPHIA* (ND Cal 1996) 948 F Supp 923. See generally §1.6. In *Playboy Enters., Inc. v Frena* (MD Fla 1993) 839 F Supp 1552, the court held that downloading copyrighted content from or uploading it to a computer bulletin board constitutes infringement of the copyright owner's right to publicly display the work. The court found that making photographs available on a BBS was a public display, even though the display was limited to subscribers and subscribers viewed the photographs only after downloading them on demand. Citing 2 Nimmer on Copyright §8.14[C] at 8-169 (1963), the court stated (839 F Supp at 1557):

> A "public display" is a display "at a place open to the public or… where a substantial number of persons outside of a normal circle of family and its social acquaintances is gathered."… A place is "open to the public" in this sense even if access is limited to paying customers.

When the Internet site operator itself is the one deciding what third party content to make available for downloading, the operator should take care to ensure that sufficient reproduction rights from the copyright owners are obtained. The United States Supreme Court in *New York Times Co., Inc. v Tasini* (2001) 533 US 483, 150 L Ed 2d 500, 121 S Ct 2381, held that the New York Times and other publishers infringed the copyrights of freelance writers by including articles in electronic databases without permission when individual articles in the databases were available for download. At the heart of the publishers' argument was the claim that an electronic version of a work is merely a revision of the original publication in which it appeared. The court disagreed, holding that the publishers were liable for copyright infringement because the databases reproduced and distributed articles standing alone and not as part of the particular collective work—the magazine or newspaper issue—to which the author contributed. See also *Video Pipeline v Buena Vista Home Entertainment, Inc.* (NJ 2002) 192 F Supp 2d 321, aff'd (3d Cir 2003) 342 F3d 191, cert denied (2004) 540 US 1178 (Internet website operator enjoined from producing its own movie trailers from clips taken from plaintiff's films on video and distributing those trailers to operator's online video retailer clients; operator's conduct infringed plaintiff's exclusive right to create derivative works, and to perform and publicly display its work, and was not protected by "first sale" or "fair use" doctrines.)

PRACTICE TIP: Copyright owners can take advantage of advanced watermarking technology to "tag" their visual images and other content with identifying information that permits them to trace images and content on other sites back to them, even if the content is altered. Copyright owners can also use site-monitoring programs to create automated logs to check for suspicious activity and advanced Internet search tools to search for infringing uses of proprietary images.

See chap 14 for information on obtaining license rights and consent to using third party content on an Internet site.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/8 Terms of Use; Online Agreements; Linking; Downloading/ C. Music on the Internet/§8.21 1. Introduction

C. Music on the Internet

§8.21 1. Introduction

The Internet and digital music technology have made public delivery of sound recordings extraordinarily fast and inexpensive. A major challenge in defending music copyrights in the Internet age is that digital music distribution technologies are constantly changing. Music can be made or captured in digital code, transferred, copied, and replayed by an ever increasing variety of means, some of which are legal, some illegal, and some untested. The recording industry has been struggling to keep pace with rapidly evolving technology through lawsuits and sponsorship of legislation.

© The Regents of the University of California

§8.22 2. Technologies

Several different technologies are currently employed to record, transfer, copy, or replay music over the Internet, including the following:

- **Streaming audio.** Streaming audio uses software known as a CODEC (short for compressor/decompressor) to pack music into a file small enough to be sent rapidly over the Internet. Usually, the music is listened to as it arrives or "streams" from a server. Streaming potentially implicates the copyright holder's right to the sound recording as well the musical work embodied in the sound recording, and potentially infringes the copyright holder's right of reproduction and right of public performance.
- **MP3.** MP3 is a software program that permits music to be recorded as a digital file and compressed using a CODEC, to facilitate uploading to the Internet, transferring from site to site, and downloading.
- **Ripping.** Ripping is the process of copying music from a CD to a hard drive using a CODEC (such as MP3) to compress the digital music so that it occupies less space on a disk and takes less time to travel over the Internet. The record industry is working on various copyright protection initiatives to make it impossible to "rip" a CD if the user has not legally purchased the disk or if the user has already "ripped" the CD a maximum number of times. Ripping implicates a copyright holder's right of reproduction.
- **Burning.** Burning refers to the act of transferring data, including music, to a CD or CD-ROM. With a CD-R (write once) or CD-RW (write multiple times) recorder, a user can easily make an exact replica of an original CD. A user can also transfer MP3 files downloaded from the Internet into a CD format and burn them onto a standard CD. As in ripping, burning implicates a copyright holder's right of reproduction.
- **Downloading.** Downloading is the process of copying a file from a site on the Internet to a hard drive. Playing a song once it has been downloaded to a hard drive can be accomplished by running a program on the computer itself (in which case the music will be heard through the computer's speakers) or by transferring the file to a portable digital player. As in ripping and burning, downloading implicates a copyright holder's right of reproduction.
- **Watermarks.** Watermark technologies are data embedded in a recording that tell a digital player device whether the user is authorized to play or replicate the music.

© The Regents of the University of California

§8.23 3. Federal Statutes

In addition to the basic prohibitions against infringement under the Copyright Act (see generally 17 USC §§501-513, discussed in §§1.1-1.21), several recent federal acts amending the Copyright Act may be implicated by the recording, copying, or transmission of music over the Internet.

© The Regents of the University of California

§8.24 a. Audio Home Recording Act of 1992 (AHRA)

The Audio Home Recording Act of 1992 (AHRA) (Pub L 102-563, 106 Stat 4237), codified primarily at 17 USC §§1001-1010, provides that importers, manufacturers, and distributors of certain digital audio recording devices must (1) file a notice and periodic statements of account with the Copyright Office (17 USC §1003(b)-(c)); (2) implement serial copyright management technology to prevent further replication of copies of the copyrighted work (17 USC §1002); and (3) pay a statutory royalty on each device and piece of media sold (17 USC §§1003-1005). The AHRA defines "digital audio recording devices" as "any machine or device of a type commonly distributed to individuals for use by individuals, whether or not included with or as part of some other machine or device, the digital recording function of which is designed or marketed for the primary purpose of, and that is capable of, making a digital audio copied recording for private use" 17 USC §1001(3). This definition includes a narrow range of devices such as digital audio tape (DAT) recorders, MiniDisc recorders, and recordable MP3 players. Multipurpose devices (devices that are not intended primarily for making digital audio copies), such as a computer or a CD-ROM drive that serves as a peripheral device for a computer, are therefore not covered. Manufacturers of covered devices receive statutory immunity from copyright infringement (17 USC §1008) but can be sued for violation of the Act (17 USC §1009). The Act also exempts consumers from liability for copyright infringement when they record music for private, noncommercial use (17 USC §1008), and provides for payment of royalties to songwriters and recording artists (17 USC §§1006-1007).

© The Regents of the University of California

§8.25 b. Digital Performance Right in Sound Recordings Act of 1995 (DPRA)

The Digital Performance Right in Sound Recordings Act of 1995 (DPRA) (Pub L 104-39, 109 Stat 336), codified primarily at 17 USC §§106(6), 111, 114-115, 119, and 801-803, extended the exclusive rights of owners of copyrights on sound recordings to public performance of the copyrighted work by means of digital audio transmission. See 17 USC §106(6). Before passage of the DPRA, sound recordings were not covered by the right of public performance. The DPRA allows copyright owners of sound recordings to license certain digital audio transmissions of their works, including subscription and interactive transmissions, and imposes statutory licenses on certain other types of digital audio transmissions of sound recordings. See 17 USC §114(d)-(f), (h). See generally *Bonneville Int'l Corp. v Peters* (ED Pa 2001) 153 F Supp 2d 763, 766, aff'd (3d Cir 2003) 347 F3d 485. Most noninteractive subscription digital audio transmissions of sound recordings are subject to statutory licensing at rates established by the Copyright Office (or else negotiated by the parties). See 17 USC §114(e)-(f). Exempt from the effect of the DPRA are traditional radio and television broadcasts and transmissions within business establishments. See 17 USC §114(d)(1). The Digital Millennium Copyright Act of 1998 (DMCA) (Pub L 105-304, 112 Stat 2860), codified primarily at 17 USC §§512, 1201-1205, and 1301-1332, is discussed in more detail in §§1.24-1.43.

As technology continued to advance, the DPRA's applicability to certain new nonsubscription digital audio services came into question. Among other things, in 17 USC §114(d)(2)-(j), the DMCA amended the statutory license provisions previously addressed by the DPRA to provide a new statutory license (at a prenegotiated standard rate) for noninteractive digital audio services (such as webcasters and digital radio services) to transmit sound recordings with the primary purpose of entertainment, if the conditions of the license are met. 17 USC §114(f) (1998). The statutory licensing scheme gives webcasters and satellite radio services access to music without need to obtain permission from each music copyright owner individually and gives record companies an efficient mechanism to receive royalties for sound recordings. For further discussion of these issues, see http://www.copyright.gov/fedreg/2000/65fr33266.html.

© The Regents of the University of California

§8.26 c. No Electronic Theft Law

The No Electronic Theft Law (NET Act) (Pub L 105-147, 111 Stat 2678) (18 USC §2311, Note) provides that sound recording infringements (including by electronic means) can be criminally prosecuted, even if no monetary profit or commercial gain is derived from the infringing activity. See 17 USC §506(a). The NET Act also amends the definition of "commercial advantage or private financial gain" to include the receipt (or expectation of receipt) of anything of value, including receipt of other copyrighted works (as in MP3 trading). See 17 USC §§101, 506(a). Punishment for such offenses includes up to three years in prison, up to $250,000 in fines, or both. 18 USC §2319(c). The NET Act extends the criminal statute of limitations for copyright infringement from 3 to 5 years. 17 USC §507(a). Regardless of whether the activity is for profit, infringers may also be civilly liable for actual damages and any lost profits or for statutory damages up to $150,000 per work infringed. 17 USC §504.

© The Regents of the University of California

§8.26A d. Internet Piracy (Pen C §653aa)

California Pen C §653aa, signed into law September 21, 2004, makes it a crime to mass-distribute a video, music, or other file on the Internet without including information that links the file to its source. Any person transmitting copies of movies, music, or games over the Internet to more than 10 people must now include his or her e-mail address or face a misdemeanor charge that could bring up to a year in prison and up to $2500 in fines. Pen C §653aa(a). Minors may be fined up to $250 for their first two offenses, and a minor's third offense may result in a $1000 fine and a year in prison. Pen C §653aa(b). The law provides exemptions for people sending works to immediate family members and for the transmission of works inside a home network. Pen C §653aa(c).

© The Regents of the University of California

§8.26B e. The Family Entertainment and Copyright Act

The Family Entertainment and Copyright Act of 2005 (Pub L 109-9, 119 Stat 218) addresses the use of file-swapping networks for piracy of films and music on the Internet by targeting some of the sources of such infringing content. The Act criminalizes the unauthorized recording of motion pictures in movie theaters, a practice of "pirates" who use camcorders to surreptitiously film new movie releases for illegal posting on file-sharing networks or for sale on the black market. 17 USC §506(a)(1)(B)-(C). The Act provides for prison terms of up to 3 years for a first offense and up to 6 years for subsequent offenses. 18 USC §2319(d)(1), (3).

The Act also addresses another trend in content piracy: the dissemination of advance copies of films and other works prior to their release date. These "pre-release" versions, such as beta versions of software or work prints of motion pictures, are another source of content for pirates. The Act provides that anyone who makes a work that the copyright owner expects to distribute commercially, but is not yet distributed, "available on a computer network accessible to members of the public" can be punished if he or she knew or should have known that the work was intended for commercial distribution. 17 USC §506(a)(1)(C). First-time offenders may be sentenced to up to 3 years in prison, or up to 5 years if they committed the offense for financial gain. 18 USC §2319(d)(1)-(2). Repeat offenders may be sentenced to up to 6 years in prison, or up to 10 years if the offense was committed for financial gain. 18 USC §2319(d)(3)-(4). Penalties apply regardless of whether the file was actually downloaded.

© The Regents of the University of California

§8.27 4. Case Law

Recording Indus. Ass'n v Diamond Multimedia. *Recording Indus. Ass'n v Diamond Multimedia* (9th Cir 1999) 180 F3d 1072, was one of the first cases to interpret the Audio Home Recording Act of 1992 (AHRA) (see §8.24). In that case, the Recording Industry Association of America sought to enjoin the manufacture and distribution of the Rio, a portable digital music player with custom software allowing a user to transfer MP3 files (see §8.22) previously downloaded from the Internet onto the user's computer hard drive to the Rio for listening elsewhere. The Ninth Circuit analyzed the language and legislative history of the AHRA, noting that, as a result of a legislative compromise with the computer industry, computers and their hard drives were expressly excluded from the AHRA. 180 F3d at 1078. The AHRA thus created a loophole that allowed pirated MP3 files to be "laundered" by passing through a computer. 180 F3d at 1079. Accord *A&M Records, Inc. v Napster, Inc.* (9th Cir 2001) 239 F3d 1004, 1024 (AHRA does not cover downloading of MP3 files to computer hard drives). The Ninth Circuit in *Recording Indus. Ass'n v Diamond Multimedia, supra,* noted that the purpose of the AHRA was to ensure that consumers had the right to make analog or digital audio recordings for their private noncommercial use, analogous to private noncommercial video cassette recordings of television programs as approved in *Sony Corp. v Universal City Studios, Inc.* (1984) 464 US 417, 78 L Ed 2d 574, 104 S Ct 774, and held that the Rio's operation was consistent with the purpose of the AHRA. The Rio merely allowed users to make copies of (and render portable or "space-shift") files that already resided on a user's hard drive. 180 F3d at 1079. The Rio was therefore not subject to the restrictions of the AHRA. 180 F3d at 1081. The Ninth Circuit's decision is important for clarifying that the AHRA itself offers little or no protection to copyright holders against online music piracy.

Bonneville Int'l Corp. v Peters. Another case of interest is *Bonneville Int'l Corp. v Peters* (3d Cir 2003) 347 F3d 485, which interpreted the Digital Performance Right in Sound Recordings Act of 1995 (DPRA) (see §8.25). Under the Copyright Act, FCC-licensed radio stations are permitted to make one royalty-free ephemeral copy of a copyrighted sound recording for purposes of broadcasting within their geographic regions. 17 USC §112(a)(1). Further, as amended by the DPRA, the Copyright Act exempts nonsubscription broadcast transmissions and retransmissions by FCC-licensed radio stations from a sound recording copyright owner's performance rights. 17 USC §114(d)(1)(A). In the *Bonneville* case, a group of radio broadcasters unsuccessfully challenged a Copyright Office rule clarifying that the exemption for royalty-free transmissions under §114(d)(1)(A) does not extend to the simultaneous transmission of radio broadcasts over the Internet via streaming audio. The court held that the Copyright Office's rule was correct and that the §114(d)(1)(A) exemption applies only to over-the-air radio broadcast transmissions and not Internet streaming of AM/FM broadcast signals. As a consequence of the Third Circuit's ruling, radio broadcasters are required to pay royalties on copyrighted sound recordings when their over-the-air broadcasts are simultaneously transmitted over the Internet.

A&M Records, Inc. v Napster. One of the most celebrated cases concerning music piracy on the Internet is *A&M Records, Inc. v Napster, Inc.* (9th Cir 2001) 239 F3d 1004. Napster operated a "peer-to-peer" ("P2P") file-sharing system that allowed users to make MP3 music files (see §8.22) stored on their individual computers available for copying by other users, to search MP3 music files located on other users' computers, and to transfer copies of other users' MP3 files from one user's computer to another over the Internet. 239 F2d at 1011. The Ninth Circuit affirmed the district court's findings that Napster users were engaging in direct copyright infringement by their wholesale reproduction and distribution of copyrighted works (see generally §§1.12-1.16), and that the fair use defense (see generally §§1.18-1.22) was not available to Napster users. Napster users were engaging in commercial use of the music files, because they were getting for free something that they would normally have to pay for and because the act of sending files to a stranger was not a personal use. 239 F3d at 1015. Their actions adversely affected the market for audio CDs and online distribution. 239 F3d at 1018. Napster users were not merely "space-shifting" music files, because the files were being distributed to the public, not merely, *e.g.,* from an individual user's computer to a portable player owned by the same user. 239 F3d at 1019. The Ninth Circuit also affirmed that Napster had both actual and constructive knowledge of its users' direct infringement, that it could have blocked access to the infringing material but did not do

so, and that it materially contributed to the infringing activity. 239 F3d at 1020. Further, Napster had a direct financial interest in the infringing activity. It was therefore likely that the plaintiffs would succeed on their claims that Napster was liable for both contributory and vicarious copyright infringement. 239 F3d at 1024. See generally §§1.13-1.16.

UMG Recordings, Inc. v MP3.Com Inc. *UMG Recordings, Inc. v MP3.Com Inc.* (SD NY 2000) 92 F Supp 2d 349 also involved use of MP3 technology. The defendant's "MyMP3.com" service was advertised as permitting subscribers to store and listen to their own music CDs from any location where they could access the Internet. To operate the service, the defendant purchased tens of thousands of popular CDs, and without authorization from plaintiff copyright owners, converted them to MP3 files (see §8.22) and stored the MP3 files on its servers. A subscriber wishing to access any of the music files was first required either to demonstrate to the defendant that he or she owned the corresponding CD by inserting the CD into his or her CD-ROM drive for a few seconds or to purchase the CD from a designated online retailer. Thereafter, the subscriber was permitted to access the MP3 file stored on defendant's server. The court held that the defendant's service infringed the plaintiffs' copyrights because the defendant was not actually replaying a stored version of a subscriber's own CD but instead was replaying converted unauthorized copies of the plaintiffs' copyrighted CDs. The court also held that the defendant could not utilize the "fair use" defense (see §§1.18-1.22) because its actions did not "transform" the original recordings and because the defendant was usurping a new derivative market for the plaintiffs' copyrighted works.

Metro-Goldwyn-Mayer Studios, Inc. v Grokster, Ltd. Yet another type of software platform for transferring music files over the Internet was at issue in *Metro-Goldwyn-Mayer Studios, Inc. v Grokster, Ltd.* (CD Cal 2003) 259 F Supp 2d 1029, aff'd (9th Cir 2004) 380 F3d 1154, vacated and remanded (2005) 545 US 913. Defendants in *Grokster* distributed free software online that enabled users to exchange music and other digital media files through peer-to-peer networks. When launched from a user's computer, the software automatically connected to the peer-to-peer network; any specified digital files (including text, video, and music) could then be shared directly with any other user connected to the same network. The software also enabled search capabilities with respect to the shared files. It was undisputed that, through file-sharing, some users were engaged in direct copyright infringement of the plaintiffs' works, although there were also substantial noninfringing uses for the defendants' software, including, *e.g.*, sharing noncopyrighted government documents or the works of William Shakespeare.

Granting the defendants' motion for summary judgment, the federal district court held that the defendants were not liable for contributory infringement (see generally §1.15), mainly because they lacked actual knowledge of the users' infringement at a time when the defendants could act to stop it. The defendants were generally aware that many users employed the software to infringe copyrighted works, but, unlike Napster, the defendants did not provide a site or facilities that materially contributed to the infringing activity. The defendants' software enabled users to share files directly, without any data being transmitted through any computers owned or controlled by the defendants.

The federal district court's decision was upheld by the Ninth Circuit Court of Appeals in *Metro-Goldwyn-Mayer Studios, Inc. v Grokster, Ltd.* (9th Cir 2004) 380 F3d 1154, vacated and remanded (2005) 545 US 913. Because the peer-to-peer file-sharing software services had substantial and commercially significant noninfringing uses, the court of appeals held that Grokster and co-defendant Morpheus could not be held liable as contributory infringers for making the software available. Further, the court of appeals held that, because Grokster and Morpheus had no control over the use of the software once they made it available, they could not be held vicariously liable for infringement.

The Supreme Court held differently. In *Metro-Goldwyn-Mayer Studios, Inc. v Grokster, Ltd.* (2005) 545 US 913, 162 L Ed 2d 781, 125 S Ct 2764, the Court overruled prior decisions and held that peer-to-peer networks could be held liable for infringing file sharing (also known as "piracy") on their networks if they intended to encourage such infringement (545 US at 913, 162 L Ed 2d at 790):

> We hold that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.

The Court found that the defendants were seeking to take advantage of the demand for music piracy following the demise of the Napster file-sharing service. 545 US at 925, 162 L Ed 2d at 793.

On remand, the district court issued a permanent injunction against defendant StreamCast Networks. The court ordered StreamCast to protect plaintiffs' copyrights "to the extent feasible" by implementing filtering to reduce the infringing capability of its Morpheus file-sharing software "while preserving its core noninfringing functionality." *MGM*

Studios, Inc. v Grokster, Ltd. (CD Cal 2007) 518 F Supp 2d 1197, 1236.

Aimster Copyright Litigation. In *In re Aimster Copyright Litig*. (7th Cir 2003) 334 F3d 643, cert denied (2004) 540 US 1107, Judge Posner affirmed a preliminary injunction for the plaintiff copyright owners against Aimster, another Internet file-sharing service. Aimster's service (which was run through instant-messaging services operated by AOL and other Internet service providers) was similar to the service offered by the defendants in *Grokster* in that Aimster did not host copies of shared music files on its own server. Aimster, however, included encryption software in its basic software package to enable the music files shared among its users to be encrypted, apparently in a deliberate effort to avoid direct knowledge of its users' infringing activities. Judge Posner held that a service provider such as Aimster that would otherwise be liable for contributory infringement cannot obtain immunity by using encryption to shield itself from actual knowledge of unlawful activities conducted over its service. Aimster had not advanced sufficient evidence to show that its service had substantial noninfringing uses.

© The Regents of the University of California

§8.28 5. RIAA Litigation Strategy

The Recording Industry Association of America (RIAA) has aggressively pursued infringement lawsuits against those it believes liable for illegally sharing music content over the Internet—including lawsuits against individuals as well as companies operating file-sharing networks. By July 2006, RIAA had reportedly filed lawsuits against 751 unnamed individuals for making copyrighted music available on file-sharing networks, continuing a campaign that has targeted a total of more than 17,000 people. For a partial list of lawsuits pending at the end of 2007, see *UMG Recordings, Inc. v Lindor* (ED NY 2007) 531 F Supp 2d 453.

An example of the success of RIAA's strategy is the holding in *BMG Music v Gonzalez* (7th Cir 2005) 430 F3d 888, cert denied (2006) 547 US 1130. The defendant downloaded 1379 copyrighted songs, purportedly intending to "sample" them, although she admitted retaining copies of 30 songs she did not purchase. BMG sought damages with respect to only the 30 songs defendant did not purchase. The court rejected the defendant's asserted fair-use defense, holding that all the downloads were illegal. The quantity of songs, the court found, was not relevant (430 F3d at 891):

> Gonzalez's claim that she obtained "only 30" (or "only 1300") copyrighted songs is no more relevant than a thief's contention that he shoplifted "only 30" compact discs, planning to listen to them at home and pay later for any he liked.

The defendant was fined $22,500, or $750 per song.

In early 2007, the RIAA launched a controversial new anti-piracy campaign on behalf of major record companies. In 2007 and continuing in 2008, the RIAA mailed hundreds of pre-litigation settlement letters to colleges and universities nationwide, informing the schools of forthcoming copyright infringement suits against one or more of their students or campus computer network personnel. The letters ask the university administrators to forward the letters to the appropriate network users to allow them an opportunity to settle the issue out of court. See RIAA press releases at: http://www.riaa.com/news_room.php.

In some cases, unrepresented defendants in RIAA lawsuits have found a sympathetic ear in federal court. See, *e.g., Elektra Entertainment Group, Inc. v O'Brien* (ND Cal, Mar. 2, 2007, No. CV 06-5289 SJO (MANx) (unpublished minute order, available at http://www.ilrweb.com/viewILRPDF.asp?filename=elektra_obrien_070302Decision. The RIAA's strategies have been actively opposed by the Electronic Frontier Foundation. See http://w2.eff.org/IP/P2P/riaa-v-thepeople.php.

© The Regents of the University of California

9

Privacy Law and Privacy Policies

I. INTRODUCTION §9.1

II. PRIVACY LAWS AFFECTING ONLINE BUSINESS §9.2
- A. How Businesses Obtain Customer Information Online
  - 1. Willing Disclosure §9.3
  - 2. Cookies §9.4
  - 3. Web Bugs §9.5
  - 4. Tracking Software §9.6
  - 5. Adware §9.6A
  - 6. Spyware §9.6B
  - 7. Phishing §9.6C
- B. Federal Privacy Laws
  - 1. United States Constitution §9.7
  - 2. Federal Legislation §9.8
    - a. Federal Trade Commission Initiatives
      - (1) Privacy Policies §9.9
      - (2) Data Security §9.9A
      - (3) Unwanted Adware §9.9B
    - b. Health Insurance Portability and Accountability Act (HIPAA)
      - (1) Privacy Aspects of HIPAA and Supporting Regulations §9.10
      - (2) Protected Health Information, Contract Requirements §9.11
    - c. Gramm-Leach-Bliley Act §9.12
    - d. Right to Financial Privacy Act §9.13
    - e. Computer Fraud and Abuse Act §9.14
    - f. Electronic Communications Privacy Act §9.15
- C. California Privacy Laws
  - 1. California Constitution §9.16
  - 2. Common Law Right of Privacy §9.17
  - 3. California Legislation §9.18
    - a. Online Privacy Protection Act (Bus & P C §§22575-22579)
      - (1) Privacy Policy Posting Requirement §9.19
      - (2) Required Contents of Privacy Policy §9.20
      - (3) Failure to Comply With Act §9.21
    - b. "Anti-Paparazzi" Statute §9.21A
    - c. Financial Information Privacy Act §9.22
    - d. California Right to Financial Privacy Act (Govt C §§7460-7493) §9.23
    - e. Required Notice of Security Breaches
      - (1) Civil Code Provisions §9.24
      - (2) Potential Safe Harbor §9.25
    - f. Civil Code §1798.83 §9.26
    - g. California Protection Against Computer Spyware Act (Bus & P C §§22947-22947.6) §9.26A
    - h. Unfair Competition Law §9.27
- D. Other States' Data Protection Programs §9.27A
- E. Special Legal Protections for Children §9.28
  - 1. Children's Online Privacy Protection Act (COPPA) §9.29
    - a. Application of COPPA §9.30
    - b. Requirements for Online Collection of Information From Children §9.31
    - c. Parental Consent §9.32
    - d. Enforcement §9.33
    - e. Safe Harbor §9.34
  - 2. Dot-Kids Act §9.35
  - 3. Kidz Privacy Website §9.36
- F. European Privacy Directive
  - 1. Scope of Directive §9.37
  - 2. Safe Harbor §9.38

III. WEBSITE PRIVACY POLICIES

A. Need for Privacy Policies §9.39
B. Content of Privacy Policies §9.40
C. Enforceability of Privacy Policies §9.41
D. Additional Resources §9.42
E. Basic Website Policy
1. Introduction §9.43
2. Form: Basic Website Privacy Policy §9.44
F. Commercial Website Policy
1. Introduction §9.45
2. Form: Commercial Website Privacy Policy §9.46

© The Regents of the University of California

§9.1 I. INTRODUCTION

The explosive growth of the Internet in the last 10 years has made it possible for detailed personal information to be collected and shared more cheaply and easily than at any time in history. Although this has produced many benefits for individuals and for society as a whole, it has also facilitated the misuse of personal information. Companies doing business on the Internet should be aware of developing privacy laws and take steps to safeguard the information they collect regarding their customers and to disclose how they handle customer information in privacy policies accessible on their websites. Identity theft and other crimes related to the misuse of personal information are on the rise, and privacy protection should be a key concern of both online businesses and their customers.

Sections 9.2-9.6 review the ways that online businesses typically obtain personal information on customers. Federal and California state privacy laws affecting online businesses are discussed in §§9.7-9.36. The European Union Privacy Directive No. 95/46/EC (Oct. 24, 1995) is reviewed in §§9.37-9.38. Sections 9.39-9.46 discuss the preparation of website privacy policies and the legal and practical concerns that should guide their drafting and implementation. A company's failure to adhere to the terms of its privacy policy or to accurately disclose its data collection and use practices has become a basis for liability under federal law, as a result of successful enforcement efforts led by the Federal Trade Commission (see §9.9), and under California law, pursuant to the California Online Privacy Protection Act of 2003 (Bus & P C §§22575-22579) (see §§9.19-9.21).

Certain privacy issues are also discussed in chap 18. For a more comprehensive discussion of federal and state privacy laws applicable in California, see Privacy Compliance and Litigation in California (Cal CEB 2008).

© The Regents of the University of California

§9.2 II. PRIVACY LAWS AFFECTING ONLINE BUSINESS

Internet privacy regulation attempts to strike a balance between customers' desires to protect their personal and financial information and the desires of companies doing business online to obtain useful data from the websites that their customers visit and the information that those customers provide. For a discussion of how companies obtain information online, see §§9.3-9.6.

Consumers are sensitive about maintaining the confidentiality of personal information provided online. This anxiety creates a barrier for companies attempting to encourage consumers to transact business online and may impede the development of online commerce. Privacy laws are therefore important in promoting the growth of e-commerce because they serve to ease consumer worries about identity theft and to protect consumer desires to not have their personal information disclosed to strangers or the government. Because protection of privacy is a vital concern for online businesses and their customers, online vendors have ample incentive to promote and endorse privacy laws and to implement website privacy policies.

NOTE: A useful discussion of identity theft and methods of combating it is available on the website of the California Office of Privacy Protection at http://www.privacy.ca.gov/identity_theft.htm.

Although efforts to enact online privacy laws at the federal level have attracted much attention, they are only now starting to result in legislation. Self-regulation is the source of most current privacy controls that influence online business practices nationally. Current federal law on website data collection is fairly sketchy, consisting largely of Federal Trade Commission (FTC) regulation and monitoring. See §9.9. By contrast, the European Union (EU) has implemented a fairly comprehensive approach to privacy regulation. See §§9.37-9.38. The EU's actions have, to some extent, induced the federal government and businesses in the United States to consider strengthening consumer privacy protections.

California has enacted the California Online Privacy Protection Act of 2003 (Bus & P C §§22575-22579), which requires commercial website operators and online services to develop and post privacy policies. For a discussion of this Act, see §§9.19-9.21.

© The Regents of the University of California

A. How Businesses Obtain Customer Information Online

§9.3 1. Willing Disclosure

When a consumer visits a website and voluntarily registers or provides personal information, the company that operates the website may simply capture and retain the information. For example, when a consumer purchases an item online, he or she typically supplies a delivery address, a credit card number, and other personal information. Although consumers usually willingly disclose this information in exchange for the convenience of shopping online, the consumer is also, at the same time, inadvertently providing information about his or her tastes and buying habits.

© The Regents of the University of California

§9.4 2. Cookies

In addition to information obtained from customers by willing disclosure, online businesses also commonly obtain information by mining data through the use of cookies, web bugs (see §9.5), or tracking software (see §9.6). These devices collect data in various ways, *e.g.,* by monitoring Internet protocol (IP) addresses.

Cookies are small pieces of data that a website places on the user's hard drive when the user visits the website. The cookie remains on the user's hard drive, so that when the user visits the same website again, the website recognizes the user as a returning guest. Cookies allow a website to store information automatically about a website user (*e.g.,* which pages the user has visited and for how long) in a file on the user's own hard drive.

Cookies and other data collection devices can be extremely useful for an online business. For example, using cookies can enable a company to determine which websites a user visited before and after it visited the company's own website. Cookies enable a business to personalize a user's computer, and thus make it more efficient for the user to conduct transactions online. The user avoids having to input the same information each time he or she returns to the same website. The site "remembers" the consumer, as well as his or her purchasing habits. Online businesses also use cookies to customize and target advertising to particular users by examining a user's web surfing patterns. For further discussion of Internet advertising, see chap 17.

By visiting a website and receiving a cookie file, a consumer may inadvertently provide information about himself or herself to the website operator. Although many consumers may not know it, their Internet browsers can be configured to block cookie files. The default settings in Internet browsers, however, usually accept cookies automatically without notifying the user.

For additional discussion of cookies, see §18.9.

© The Regents of the University of California

§9.5 3. Web Bugs

In addition to cookies (see §9.4), a business may passively collect data from a computer user through the use of "web bugs." Web bugs are very small graphic image files. They are implanted in a web page and are usually the same color as the background and therefore invisible to the computer user. A web bug can send various information back to its own server such as the IP address of the computer that downloaded the page with the implanted bug, the Uniform Resource Locator (URL) of the page, when the page was viewed, the kind of browser on the computer, and whether there is a cookie on the computer placed there by the same server.

© The Regents of the University of California

§9.6 4. Tracking Software

Online businesses often use tracking software to collect information about customers. The tracking software may be included in other downloaded software programs that are designed to help customers, *e.g.,* download music or speed up downloads. Some tracking software traces a consumer's web surfing path and returns the information to the company that distributed the software. When a particular user purchases and then downloads a software program, he or she may give the software vendor personal information in connection with the purchase transaction. Information gleaned later by the tracking software can then be linked to the particular user who purchased the software program.

The FTC requires that use of tracking software be adequately disclosed. For example, the FTC brought charges against Sears Holdings Management Corporation (SHMC) for failing to disclose that it used tracking software in connection with its sears.com and kmart.com websites to monitor users' Internet activities. The settlement agreement requires SHMC to cease collecting data using tracking software installed before the settlement, prominently inform existing users that SHMC software was tracking their Internet use, assist users in uninstalling the tracking software, destroy any information collected, and obtain express user consent to the download or installation of any future tracking software. See *In re Sears Holdings Mgmt. Corp.* (June 4, 2009) FTC File No. 082 3099 (see http://www.ftc.gov/os/caselist/0823099/090604searsagreement.pdf).

Some federal courts have held that because IP addresses identify computers and not people, they are not personally identifiable information. See, *e.g., Johnson v Microsoft Corp.* (WD Wash, June 23, 2009, No. C06-0900RAJ) 2009 US Dist Lexis 58174 (collecting IP addresses as part of operating system update did not breach license agreement prohibition on transmitting personally identifiable information). However, the New Jersey Supreme Court held that Internet service providers are forbidden from disclosing subscriber IP addresses without a subpoena. *State v Reid* (NJ 2008) 945 A2d 26. Similarly, under the EU Data Protection Directive (see §§21.11-21.13), IP addresses may be considered to be personal information.

For additional discussion of tracking software, see §§18.6, 18.10.

© The Regents of the University of California

§9.6A 5. Adware

"Adware" refers to software programs that result in unwanted delivery of advertisements to a computer user's desktop or Internet browser, often in the form of pop-up ads or other intrusive and disruptive forms of online electronic advertising. Adware is often installed without a user's knowledge or consent, and typically depends on tracking software or other forms of user monitoring to determine which ads to deliver to a particular user and when to deliver them. For some users, adware may be a necessary evil of accessing certain desirable software programs or online services (*e.g.,* websites that require users to view advertisements in order to access certain content), but more often adware is an unwanted and unexpected nuisance that installs itself deviously and sometimes illegally (see discussion of FTC initiatives in §9.9) and can be difficult to locate and remove.

© The Regents of the University of California

§9.6B 6. Spyware

Spyware is a term frequently used to describe especially pernicious forms of tracking software. Spyware surreptitiously gathers information about a computer user or co-opts system resources and redirects them toward uses of which the user is unaware and to which the user has not consented, *e.g.,* serving unsolicited e-mail and launching "denial of service" attacks. One online definition of "spyware" reads as follows (http://www.webopedia.com/terms/spyware.html):

> Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.

Like spam before it, spyware is the subject of much scrutiny and increasing regulatory focus as remedying the problems it causes consumes ever increasing numbers of hours. California, taking a leading role in legislative efforts to combat spyware, has enacted the Consumer Protection Against Computer Spyware Act (Bus & P C §§22947-22947.6), discussed in §9.26A.

© The Regents of the University of California

§9.6C 7. Phishing

"Phishing" refers to the practice of sending out millions of e-mails bearing what appears to be the return address of a legitimate entity such as a bank, credit card company, or retailer, and asking the recipient to supply or update associated personal and financial information. E-mail addresses are gathered from public Internet postings and by other automated means of searching the Internet, including spyware, crawlers, and robots. An e-mail recipient who complies with the request for information provides the sender with information that can be used to invade the recipient's privacy for financial or other reasons.

The California Anti-Phishing Act of 2005 (Bus & P C §§22948-22948.3 provides for damages of up to $500,000 to owners of websites, trademarks, or companies that provide Internet service that are adversely affected. Bus & P C §22948.3(a)(1). Individuals directly affected may seek injunctive relief and damages up to $5000 per phishing violation. Bus & P C §22948.3(a)(2).

NOTE: In June 2007, a "phishing scheme" that enabled a California man to appropriate AOL subscribers' personal and credit card information resulted in the first jury conviction under the CAN-SPAM Act. A Central District judge sentenced the perpetrator to 70 months in prison and fines of more than $1 million. See http://www.justice.gov/usao/cac/pressroom/pr2007/079.html.

For more on phishing, see http://www.webopedia.com/DidYouKnow/Internet/2005/phishing.asp.

© The Regents of the University of California

B. Federal Privacy Laws

§9.7 1. United States Constitution

A right of privacy is not directly expressed in the United States Constitution or the Bill of Rights. Nevertheless, the Supreme Court has held that privacy is implicitly protected by the Constitution. See *Lawrence v Texas* (2003) 539 US 558, 156 L Ed 2d 508, 123 S Ct 2472; *Roe v Wade* (1973) 410 US 113, 35 L Ed 2d 147, 93 S Ct 705. See also *Fugate v Phoenix Civil Serv. Bd.* (9th Cir 1986) 791 F2d 736.

In a matter of first impression, the Ninth Circuit recently held that computer monitoring that reveals website IP addresses and e-mail addresses does not implicate the Fourth Amendment. *U.S. v Forrester* (9th Cir 2008) 512 F3d 500. The court's analysis followed the reasoning in *Smith v Maryland* (1979) 442 US 735, 61 L Ed 2d 220, 99 S Ct 2577, in which the Supreme Court held that use of information generated by a pen register does not implicate the Fourth Amendment prohibition of warrantless searches.

© The Regents of the University of California

§9.8 2. Federal Legislation

Privacy legislation at the federal level has been piecemeal and industry-specific. Self-regulation is the principal source of most privacy controls that influence online business practices nationwide. In the absence of comprehensive federal privacy legislation, the Federal Trade Commission (FTC) has mounted several privacy initiatives based on its general authority under the FTC Act to regulate unfair business practices (see §9.9). Beyond the general enforcement efforts of the FTC, federal legislative initiatives have mainly focused on the protection of children. See §§9.28-9.36. In addition, the Health Insurance Portability and Accountability Act of 1996 (Pub L 104-191, 100 Stat 1936) (see §§9.10-9.11) and the Gramm-Leach-Bliley Act (Pub L 106-102, 113 Stat 1332) (see §9.12) include provisions concerning online data collection and use, and practitioners with clients in the health or financial services industries should familiarize themselves with these acts.

Personal information regarding adult consumers in the possession of nongovernmental entities is generally unregulated under federal law, with the exception of health and financial information (see §§9.10-9.12), records of video rentals (see 18 USC §2710), information about cable television subscribers (see 47 USC §551), customer-use information in telecommunications (see 47 USC §222), and student records (see 20 USC §1232g).

© The Regents of the University of California

a. Federal Trade Commission Initiatives

§9.9 (1) Privacy Policies

The Federal Trade Commission (FTC) has implemented several privacy initiatives, including efforts to hold online companies to the promises they make in their privacy policies. See generally http://www.ftc.gov/privacy. As a result, a company risks liability for failure to adhere to the terms of its privacy policy or to accurately disclose its data collection and use practices. See 15 USC §45(a) (prohibiting unfair or deceptive trade practices). Because privacy policies are now an expected element of any reasonably sophisticated website, prudent business practice counsels adherence to their terms. Company privacy policies are discussed in §§9.39-9.46.

The FTC has successfully undertaken a number of enforcement actions in recent years based on companies' failure to adhere to the terms of their own privacy policies. *In re GeoCities, a Corp.* (Feb. 5, 1999) No. C-3850 (see http://www.ftc.gov/os/caselist/c3850.htm) was the first public example of a company held accountable for such a failure. GeoCities operated an online "virtual community" that organized web pages created by GeoCities' millions of members into themed "neighborhoods" and was, at the time, one of the most popular sites on the World Wide Web. In its complaint, the FTC accused GeoCities of misrepresenting the purposes for which it was collecting personal information from children and adults. In settling with the FTC, GeoCities agreed to post a clear and prominent privacy notice on its site, including a description of what information was being collected and for what purpose, to whom it would be disclosed, and how a user could access and remove the information if desired. In addition, to assist parents in monitoring children's Internet activities, GeoCities agreed to obtain a parent's consent before collecting any information from children under the age of 13.

As companies with existing privacy policies have taken steps to revise those policies to accommodate changing business practices or to keep up with evolving technology, the FTC has broadened the scope of its enforcement actions to address the manner in which companies implement these revisions. In July 2004, the FTC initiated and settled what it described as "the first case to challenge deceptive and unfair practices in connection with changes that a company makes to its privacy policy." *In re Gateway Learning Corp.* (July 7, 2004) FTC File No. 042-3047 (see http://www.ftc.gov/opa/2004/07/gateway.htm). According to FTC allegations, Gateway Learning Corp. (Gateway), which had collected personal information from its customers and website visitors, then changed its privacy policy to permit Gateway to share that information with third parties without obtaining consent or notifying the affected consumers. Gateway marketed and sold "Hooked on Phonics" products through its http://www.hop.com website. It had a privacy policy that, since the year 2000, stated that Gateway did not sell, rent, or loan personally identifiable information without the consumer's consent, and that, in the event of any change to the policy, consumers would have the chance to opt out of any disclosure of personally identifiable information. The FTC alleged that, in April 2003, Gateway began renting consumers' personal information to marketing companies, and that consumers were not notified or given an opportunity to opt out. Under the terms of its settlement with the FTC, Gateway was prohibited from misrepresenting how it uses data that it collects, and was further prohibited from sharing any personal information unless a consumer had specifically opted into the sharing. The Consent Order also provided that future material changes to Gateway's privacy policy could not apply retroactively without consumers' consent and Gateway was required to forfeit the $4600 it had earned by renting the personal information.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/9 Privacy Law and Privacy Policies/§9.9A (2) Data Security

§9.9A (2) Data Security

FTC proceedings. The FTC is also turning its attention to companies that fail to implement adequate and appropriate security measures to protect online information. In *In re Educ. Research Ctr. of Am., Inc.* (May 9, 2003) No. C-4079 (see http://www.ftc.gov/os/caselist/c4079.htm), the FTC ordered a company collecting and selling information from students as young as 10 years old to destroy all information from children under 13 and refrain from using data for noneducational marketing without disclosing its intended use.

In *In re Petco Animal Supplies, Inc.* (Nov. 8, 2004) No. 032-3221 (see http://www.ftc.gov/os/caselist/0323221/0323221.htm), Petco agreed to settle charges that, as a result of security flaws with its http://www.petco.com website, Petco violated federal law by failing to uphold privacy promises made to its customers. Apparently, the Petco website was vulnerable to attacks by hackers, leading to unauthorized access of personal information about Petco customers. According to the FTC, reasonable security measures would have avoided those attacks. Under the terms of the settlement, Petco agreed to implement a 20-year program for the security of personal information at its website. See also *In re DSW Inc.* (Dec. 1, 2005) No. 052-3096, available at http://www.ftc.gov/os/caselist/0523096/0523096.htm.

In *In re Genica Corp.* (Feb. 5, 2009) FTC File No. 082 3113 (see http://ftc.gov/os/caselist/0823113/090125genicaagree.pdf), the company collected and stored personal information of customers purchasing consumer electronics through its geeks.com website. The data, allegedly stored in clear, readable, unencrypted text, was breached and stolen by hackers. The FTC claimed Genica did not use "reasonable" or "appropriate" data protection measures. Moreover, the geeks.com website stated that security and controls were used to safeguard personal information. The FTC alleged that these statements were false and misleading in violation of the FTC Act. Under the terms of the FTC settlement, Genica is required to implement an information security program and obtain independent third party audits of the program every 2 years for 10 years.

ChoicePoint settlement. In January 2006, the FTC announced the largest civil fine in FTC history, as consumer data broker ChoicePoint, Inc. agreed to pay $10 million in civil penalties to the FTC and $5 million in consumer redress as part of its agreement with the FTC to settle charges that the company had violated federal laws and consumers' privacy rights through its security and record-handling procedures. *U.S. v ChoicePoint, Inc.* (Jan. 26, 2006) FTC File No. 052-3069 (see http://www.ftc.gov/os/caselist/choicepoint/choicepoint.htm). According to the FTC, ChoicePoint obtained and sold personal information of consumers, including their names, Social Security numbers, birth dates, employment information, and credit histories, to more than 50,000 businesses. See http://www.ftc.gov/opa/2006/01/choicepoint.htm. ChoicePoint acknowledged that the personal financial records of more than 163,000 people in the ChoicePoint database had been compromised, leading to at least 800 cases of identity theft.

In its complaint against ChoicePoint, the FTC alleged violations of the FTC Act and of the Fair Credit Reporting Act (15 USC §§1681-1681x) based on allegations that ChoicePoint lacked reasonable screening procedures and disclosed sensitive personal information to subscribers whose applications should have raised obvious concerns. Moreover, law enforcement officials had notified ChoicePoint of fraudulent subscriber activity as early as 2001.

Under the terms of the settlement agreement, ChoicePoint agreed not to furnish consumer reports to anyone not having a permissible purpose for the reports, and to establish and maintain procedures to ensure that consumer reports would not be furnished to anyone not having a permissible purpose for the reports. ChoicePoint was ordered to verify the identity of businesses that apply to receive reports and to audit the usage of the reports by the recipients. In order to provide for better protection of consumer information in ChoicePoint's possession, ChoicePoint also agreed to establish, implement, and maintain a comprehensive information security program designed to protect the security, confidentiality, and integrity of the personal information it collects from or about consumers. ChoicePoint is required to have its security program audited every 2 years for the next 20 years to confirm that the program complies with the terms of the settlement agreement. See also *In re CardSystems Solutions, Inc.* (Feb. 23, 2006) FTC File No. 0523148 (see http://www.ftc.gov/os/caselist/0523148/0523148consent.pdf) (failure to provide reasonable security for sensitive consumer information led to "largest known compromise of financial data to date," resulting in millions of dollars of

fraudulent purchases; settlement requires comprehensive protection program and 20-year audit requirement).

FTC Red Flags Rule. As part of the Fair and Accurate Credit Transactions (FACT) Act of 2003 (Pub L 108-159, 117 Stat 1952), the FTC promulgated the "Red Flags Rule," which requires financial institutions and creditors to develop and implement written identity theft prevention programs. See 16 CFR §681.2(d); http://www.ftc.gov/redflagsrule. The programs must provide for the identification, detection, and response to patterns, practices, or specific activities—known as "red flags"—that could indicate identity theft has occurred. 16 CFR §681.2(b)(9). For purposes of the rule, a "creditor" is any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit. 15 USC §1691a(e). Accepting credit cards as a form of payment does not in and of itself make an entity a "creditor." Examples of "creditors" include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. 16 CFR §681.2(b)(5). When nonprofit and government entities defer payment for goods or services, they, too, may be considered creditors. 15 USC §1691a(d). The Red Flags Rule is currently scheduled to go into effect on June 1, 2010. http://www.ftc.gov/opa/2009/10/redflags.shtm. In *American Bar Ass'n v FTC* (D DC 2009) 671 F Supp 2d 64, the federal district court enjoined the FTC from enforcing the Red Flags Rule against attorneys.

© The Regents of the University of California

§9.9B (3) Unwanted Adware

The FTC has also tackled the problem of unwanted adware, including the undisclosed presence of adware in, or bundled with, other software programs. In *In re Advertising.com, Inc.* (Sept. 12, 2005) No. 042-3196 (see http://www.ftc.gov/os/caselist/0423196/0423196.htm), Advertising.com, a subsidiary of America Online, agreed to settle charges that it violated federal law by failing to disclose that it had bundled adware with free software offered to consumers. Advertising.com had offered consumers a security program called SpyBlast for free, without disclosing that SpyBlast included adware that tracked users' online activities, and then used information obtained from that tracking to deliver pop-up ads to those users. Because the presence of bundled adware would be material to a user's decision whether or not to download SpyBlast, the FTC alleged that the failure to disclose was material. Under the settlement agreement, Advertising.com was prohibited from making any claims about SpyBlast or any other software promoted as security software unless the presence and effects of any bundled adware were clearly and conspicuously disclosed. Advertising.com also agreed to certain ongoing recordkeeping requirements, and to permit the FTC to monitor its compliance with the settlement agreement.

© The Regents of the University of California

b. Health Insurance Portability and Accountability Act (HIPAA)

§9.10 (1) Privacy Aspects of HIPAA and Supporting Regulations

Although limited to health information, the privacy aspects of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub L 104-191, 100 Stat 1936) represent an important step in the development of privacy laws in the United States. Intended in part to streamline and set standards for the electronic exchange of health care information for the benefit of consumers, HIPAA raised concerns about the privacy of medical records in all forms, including those maintained and transmitted electronically. In response, the U.S. Department of Health and Human Services issued the Privacy Rule (45 CFR pt 160, pt 164, subpts A, E; see §9.11), which governs access to and use of protected health information by patients and others, and the Security Rule (45 CFR pts 160, 162, 164), which defines the physical and technical safeguards that protect information in electronic form. HIPAA does not preempt state laws that provide stronger privacy protections for consumer health care information.

Information on HIPAA implementation in California is available at the California Office of Health Information Integrity (CalOHII) website, http://www.ohi.ca.gov/calohi. In addition, the United States Department of Health and Human Services website at http://www.hhs.gov/ocr/hipaa provides links to information about HIPAA.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/9 Privacy Law and Privacy Policies/§9.11 (2) Protected Health Information, Contract Requirements

§9.11 (2) Protected Health Information, Contract Requirements

The Privacy Rule (45 CFR pt 160, pt 164, subpts A, E), part of the administrative regulations implementing HIPAA (see §9.10), governs handling of patient health care information by health plans, health care clearinghouses, and health care providers that transmit health information in electronic form. 45 CFR §160.102. The Privacy Rule limits the disclosure of an individual's health information, including "past, present, or future payment for the provision of health care" (45 CFR §160.103) to the minimum necessary.

A "business associate" is a person or an entity contracted to provide "legal, actuarial, accounting, consulting… or financial services" to a covered entity. 45 CFR §160.103. A covered entity may disclose only the minimum information necessary for a business associate to complete its assigned task, and must develop policies to determine which members of its workforce need access to protected health information to do their jobs. 45 CFR §164.502(b).

Contracts between covered entities and their business associates that require disclosure of protected health information must describe the protected health information to be made available to a business associate and the limitations on its use. 45 CFR §164.504(e)(1). The contract must also require that a business associate implement measures to prevent disclosure or use of the information—by itself or its agents—for purposes other than those specified by the contract. 45 CFR §164.504(e)(2). A covered entity that discovers a business associate has violated the contract privacy provision is obligated to try to cure the breach; alternatively, the covered entity may terminate the contract or report the problem to the U.S. Department of Health and Human Services. 45 CFR §164.504(e)(1). More information is available at http://www.hhs.gov/ocr/privacy/index.html.

© The Regents of the University of California

§9.12 c. Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Financial Modernization Act of 1999 (Pub L 106-102, 113 Stat 1338) regulates the handling of nonpublic consumer information by financial institutions. Title V of the Act (15 USC §§6801-6827) is devoted to privacy issues; it addresses disclosure of and fraudulent access to consumer information and authorizes the FTC and other agencies to formulate rules to implement privacy provisions. 15 USC §6804. The Act requires that privacy statements be disclosed by financial institutions and restricts their ability to disclose nonpublic personal information about consumers to third parties. See 15 USC §6801-6809. See also 15 USC §6805(a) ("financial institution" defined). In response to criticism that privacy notices were too lengthy and complex and a finding that most consumers did not read or understand the notices, six of the federal agencies that enforce the Act (the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the FTC, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission) undertook a "Form Development Project" to develop a prototype privacy notice. The prototype was released as part of a report entitled "Evolution of a Prototype Financial Privacy Notice," available at http://www.ftc.gov/privacy/privacyinitiatives/ftcfinalreport060228.pdf. See also http://www.ftc.gov/opa/2006/03/jointprprivacy.htm (FTC press release announcing availability of report). Phase two of the project will measure the effectiveness of the prototype notice as compared to other types of notices.

Implementing regulations of the Act include the Safeguards Rule (16 CFR §314.1(a)), which sets forth standards to protect the confidentiality of customer information acquired by financial institutions. Its provisions address the responsibilities of "service providers," and define a "service provider" as an individual or entity that "receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution." 16 CFR §314.2(d).

The Safeguards Rule requires a financial institution to designate an employee to coordinate security of protected information, identify risks that could result in the release of confidential customer information, and assess the adequacy of the safeguards imposed. 16 CFR §314.4. Financial institutions must retain service providers that will similarly safeguard consumer information and that will insist their subcontractors also pledge to adequately safeguard protected information. 16 CFR §314.4(d)(1)-(2).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/9 Privacy Law and Privacy Policies/§9.13 d. Right to Financial Privacy Act

§9.13 d. Right to Financial Privacy Act

Under the Right to Financial Privacy Act of 1978 (RFPA) (12 USC §§3401-3422), no financial institution may disclose to a government authority information contained in the financial records of a customer, unless the customer has consented, or unless the disclosure is in response to a subpoena or search warrant. See 12 USC §§3402, 3404-3408. In addition, an institution may not require a customer to waive his or her right as a condition of doing business with it. 12 USC §3404(b). The RFPA also restricts the use of information that a government agency has obtained, *e.g.,* the information may not be transferred to or exchanged with other agencies. 12 USC §3412. For discussion of the California statutory equivalent to the RFPA, see §9.23.

© The Regents of the University of California

§9.14 e. Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA) (18 USC §1030) addresses computer crimes such as hacking. It defines a series of computer-related crimes, including intentionally accessing a computer without authorization (or exceeding authorized access) and thereby obtaining confidential information or anything of value, perpetrating a fraud, or causing other damage. See 18 USC §1030(a). In addition to criminal penalties, the statute creates a private right of civil action for any person who suffers damages or loss from a violation of the Act. See 18 USC §1030(g). For further discussion of the CFAA, see §§18.3-18.7.

© The Regents of the University of California

§9.15 f. Electronic Communications Privacy Act

The Electronic Communications Privacy Act of 1986 (ECPA) (Pub L 99-508, 100 Stat 1848), codified at 18 USC §§2510-2522 and 2701-2712, expanded the scope of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (also known as the Wiretap Act) (Pub L 90-351, 82 Stat 211) to prohibit the unauthorized interception, use, and disclosure of electronic, as well as oral and wire, communications.

The ECPA has two parts: Title I, codified at 18 USC §§2510-2522, which continues to be known as the Wiretap Act, covers interception of oral, wire, and electronic communications. Significantly, Title I of the ECPA does not cover *stored* electronic communications. Title II of the ECPA, codified at 18 USC §§2701-2712, also known as the Stored Communications Act (SCA), covers unauthorized access to wire and electronic communications and transaction records held in storage.

In addition to criminal penalties, Title I of the ECPA creates a private right of action against anyone who, without proper authorization, "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 USC §§2511(1)(a), 2520. The element of intent is important, and it is defined narrowly. As used in the ECPA, it means "more than that one voluntarily engaged in the conduct or caused the result. Such conduct or the causing of the result must have been the person's conscious objective." *In re Pharmatrak, Inc. Privacy Litig.* (D Mass 2003) 292 F Supp 2d 263, 266 (granting summary judgment for defendant based on lack of requisite intent).

In *Fraser v Nationwide Mut. Ins. Co*. (3d Cir 2003) 352 F3d 107, the Third Circuit held that Title I of the ECPA did not prohibit an employer from searching an employee's e-mail lodged on the employer's file server, because no contemporaneous "intercept" of the e-mail had occurred. The court also held that the employer qualified for the exception to liability under Title II of the ECPA provided by 18 USC §2701(c)(1) for searches by communication service providers, because the employer administered its own e-mail system on which the employee's e-mail was stored.

In *Quon v Arch Wireless* (9th Cir 2008) 529 F3d 892, cert granted sub nom *City of Ontario v Quon* (2009) ___ US ___, 175 L Ed 2d 617, 130 S Ct 1011, the Ninth Circuit held that employees have an expectation of privacy in text messages sent and received on city-owned pagers, and that a wireless provider violated the SCA by releasing the transcripts of employee text messages to their employer, the Ontario Police Department. Although the police department had a general "Computer Usage, Internet and E-mail Policy" giving the city the right to monitor e-mail traffic and clarifying that employees had no right to privacy in their city e-mail accounts, the policy did not address text messages. 529 F3d at 896. The defendant was an electronic communications service under the SCA because it provided a service enabling the employees to send and receive messages, as distinct from merely storing the messages. Therefore, in the absence of an agreement to the contrary, consent from the employees was required in order to release the transcripts. 529 F3d at 901.

PRACTICE TIP: Generally, employers should be counseled to have employees sign acknowledgments that company computers, telephones, mobile phones, pagers, networks, and e-mail facilities are company property, and that employees do not have any expectation of privacy in their e-mail, text messages, or other communications using devices or facilities the employer owns, subscribes to, or pays for. But see *U.S. v Ziegler* (9th Cir 2007) 474 F3d 1184 (employees retain at least some expectation of privacy in their offices under Fourth Amendment; however, employer may consent to search).

The ECPA is discussed further in §§18.8-18.13.

© The Regents of the University of California

C. California Privacy Laws

§9.16 1. California Constitution

Although not expressed in the United States Constitution, a right to privacy is set forth in the California Constitution (Cal Const art I, §1):

> All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.

Whether an individual's constitutional right to privacy has been violated depends first on whether that individual had a personal and objectively reasonable expectation of privacy that was infringed. Once an expectation of privacy is established, the next inquiry is whether that expectation was infringed by unreasonable intrusion. In the context of workplace computer and Internet use, courts rarely get beyond the first prong of this analysis, finding that employees do not have a reasonable expectation of privacy sufficient to justify a claim of invasion of privacy. *TBG Ins. Servs. v Superior Court* (2002) 96 CA4th 443, 117 CR2d 155 (employee working at home using computer supplied by employer had no reasonable expectation of privacy with regard to use of employer's computer).

Internet users have brought cases under the California constitution alleging that online practices such as cookies, web bugs, and other means for tracking users' online behavior violate the state constitutional right to privacy. See Saunders, *Trial Date Set in DoubleClick Case*, June 13, 2001, available at http://www.clickz.com/showPage.html?page=784391. For discussion of the use of cookies, web bugs, tracking software, adware, and spyware, see §§9.4-9.6B.

© The Regents of the University of California

§9.17 2. Common Law Right of Privacy

A common law right of privacy exists under California law. *Hernandez v Hillsides* (2009) 47 C4th 272, 97 CR3d 274; *Shulman v Group W Prods., Inc.* (1998) 18 C4th 200, 74 CR2d 843. The four traditional common law privacy torts include:

- Intrusion into a person's solitude or seclusion;
- Publicity that puts a person in a false light;
- Public disclosure of embarrassing private facts; and
- Commercial appropriation of a person's name or likeness.

For a detailed discussion of the elements of each of these torts, as well as defenses to them, see California Business Litigation, chap 11 (Cal CEB 2002). For further discussion of tort-law remedies for invasions of privacy that occur online or through the use of online resources, see chap 20.

A common law negligence cause of action may also apply if an entity mishandles personal data collected on its systems. In *Ruiz v Gap, Inc.* (ND Cal 2008) 540 F Supp 2d 1121, the plaintiff submitted an online application for employment with the Gap, including personal information such as his Social Security number. Two laptop computers containing the unencrypted Social Security numbers of approximately 800,000 GAP job applicants were stolen. The court held that the plaintiff could sustain a legal action for negligence despite the fact that he had not yet incurred any specific harm other than being placed at an increased risk of identity theft. The court held that being at an increased risk of identity theft is sufficient to constitute an "injury in fact." 540 F Supp 2d at 1126.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/9 Privacy Law and Privacy Policies/§9.18 3. California Legislation

§9.18 3. California Legislation

California has taken a leading role among the states in regulating online privacy. Numerous statutory provisions protect certain information and proscribe specific types of invasions of privacy in California, both on and off the Internet. They include:

- California Anti-Phishing Act of 2005 (Bus & P C §§22948-22948.3) (see §9.6C);
- California Online Privacy Protection Act of 2003 (Bus & P C §§22575-22579) (see §§9.19-9.21);
- California Financial Information Privacy Act (Fin C §§4050-4060 (see §9.22);
- California Right to Financial Privacy Act (Govt C §§7460-7493) (see §9.23);
- Civil Code §§1798.29, 1798.82-1798.84 (duty to give consumer notice of breach of online security; see §§9.24-9.25);
- Consumer Protection Against Computer Spyware Act (Bus & P C §§22947-22947.6) (see §9.26A);
- California's Unfair Competition Law (Bus & P C §§17200-17210) (see §9.27);
- California Invasion of Privacy Act (Pen C §§630-637.6) (use of listening devices and techniques);
- Civil Code §3344 (commercial appropriation of another's name, voice, signature, photograph, or likeness);
- Civil Code §985 (private writings);
- Information Practices Act of 1977 (CC §§1798-1798.78) (personal and confidential information protected, authorizing civil actions if agency modifies, transfers, or destroys any record containing personal information to avoid compliance with any provisions of Act);
- Civil Code §1798.81.5 (businesses must take reasonable measures to protect personal information in their possession and personal information they disclose to third parties from "unauthorized access, destruction, use, modification or disclosure");
- Civil Code §1798.83 (obligation of businesses that have disclosed certain personal information to third parties for direct marketing purposes to provide, on request, a list of the categories of information disclosed and the names and addresses of such third parties) (see §9.26);
- Consumer Credit Reporting Agencies Act (CC §§1785.1-1785.43) (consumer credit reports);
- Investigative Consumer Reporting Agencies Act (CC §§1786-1786.56) (reports of character, reputation, personal characteristics, and mode of living);
- Civil Code §1798.91 (prohibits businesses and health care providers from disclosing medical information for direct marketing purposes without express authorization of the patient);
- Education Code §§67140-67147.5 (privacy of student records); and
- Confidentiality of Medical Information Act (CC §§56-56.37).

© The Regents of the University of California

a. Online Privacy Protection Act (Bus & P C §§22575-22579)

§9.19 (1) Privacy Policy Posting Requirement

The California Online Privacy Protection Act of 2003 (Bus & P C §§22575-22579) requires an operator of a commercial website or online service that collects "personally identifiable information" from customers who are California residents to post its privacy policy on its website or online service and to comply with that policy. See Bus & P C §§22575(a), 22576.

For purposes of the Act, "personally identifiable information" means individually identifiable information about a consumer that is collected online and includes the consumer's name, address, e-mail address, telephone number, and Social Security number, as well as other identifiers that permit him or her to be contacted physically or online, and information collected and maintained in combination with the specified identifiers. Bus & P C §22577(a)(1)-(7).

The Act's requirement that the operator "conspicuously post" its privacy policy means that it must post the policy through any of these means (Bus & P C §22577(b)(1)-(5)):

- On the operator's home page or the first significant page after entering the website;
- Through an icon that hyperlinks to the actual policy, if the icon is located on the operator's home page or the first significant page after entering the website, and the icon contains the word "privacy" and is a contrasting color from the web page where it is located;
- Through a hyperlink to the actual policy if the link is located on the operator's home page or the first significant page after entering the website, and the link includes the word "privacy," is in capital letters at least as big as the surrounding text, and is in larger type than the surrounding text, or contrasting type, or set off by symbols or other marks;
- Through any other functional hyperlink that a reasonable person would notice; or
- For an online service, any other reasonably accessible means of making the privacy policy available for customers.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/9 Privacy Law and Privacy Policies/§9.20 (2) Required Contents of Privacy Policy

§9.20 (2) Required Contents of Privacy Policy

The privacy policy required under these provisions must (Bus & P C §22575(b)(1)-(4)):

- Identify the categories of personally identifiable information the operator collects through the website about individuals who visit the site and the third persons or entities with whom the operator may share the information;
- Describe any process the operator maintains for an individual to review and request changes to any of his or her information;
- Describe how the operator notifies visitors to the website of material changes to the privacy policy; and
- Indicate the policy's effective date.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/9 Privacy Law and Privacy Policies/§9.21 (3) Failure to Comply With Act

§9.21 (3) Failure to Comply With Act

Under the California Online Privacy Protection Act of 2003 (Bus & P C §§22575-22579), an operator who fails to post its privacy policy with 30 days after being notified of noncompliance or who fails to comply with the provisions of its privacy policy is in violation of these provisions. Bus & P C §§22575(a), 22576. The operator's failure to comply must be either (a) knowing and willful or (b) negligent and material. Bus & P C §22576(a)-(b).

NOTE: Although it indicates what constitutes noncompliance with its provisions, the Act does not specify what entity or agency will notify operators of noncompliance or any penalties for noncompliance.

© The Regents of the University of California

§9.21A b. "Anti-Paparazzi" Statute

California's "anti-paparazzi" law, CC §1708.8, generally creates liability for either physical or constructive invasion of privacy when a person knowingly either enters someone's land without permission or otherwise attempts to capture in an offensive manner "any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal or familial activity under circumstances in which the plaintiff had a reasonable expectation of privacy." CC §1708.8(a)-(b). See *Turnbull v American Broadcasting Cos.* (CD Cal, 2004) 2004 US Dist Lexis 24351, *72 (statute "intended to prevent paparazzi, photographers or other journalists from invading the privacy of individuals and then selling the images unlawfully obtained by stealth"). In 2009, the statute was amended to broaden its reach. As a result, any transmission, publication, broadcast, or other use of any unlawfully obtained image, recording, or impression also violates CC §1708.8 if made with actual knowledge that the image, recording, or impression was obtained unlawfully—unless the defendant provides compensation to the person whose privacy rights were violated. CC §1708.8(f). Violators may be liable for punitive damages as well as up to three times the amount of any general and special damages, and may also be required to disgorge any profits obtained from the violation. CC §1708.8(d)-(e).

© The Regents of the University of California

§9.22 c. Financial Information Privacy Act

The California Financial Information Privacy Act (Fin C §§4050-4060) requires financial institutions to obtain permission from customers before sharing customer information with certain third parties. See Fin C §4053(a).

The legislature intended that this Act take advantage of the explicit permission granted to the states by the Gramm-Leach-Bliley Act (see §9.12) to enact privacy protections stronger than those in federal law. See Fin C §4051.5(a)(4). Businesses operating in the financial services sector should be aware the provisions of this Act and take steps to comply with its provisions.

Generally, the Act requires financial institutions to obtain written consent from a consumer before sharing the consumer's nonpublic personal financial information, including information collected online. It permits the consumer to direct the financial institution to not share the information with affiliated companies or other companies with whom the institution has contracted to provide financial services. See Fin C §§4053, 4053(a)(2), 4052.5.

© The Regents of the University of California

§9.23 d. California Right to Financial Privacy Act (Govt C §§7460-7493)

Similar to the California Financial Information Privacy Act (see §9.22), the California Right to Financial Privacy Act (Govt C §§7460-7493) requires financial institutions to obtain permission from customers before sharing customer information with certain third parties. Under the Act, a financial institution may not disclose the financial records of any customer to a state or local agency unless the customer has given his or her consent or in response to a subpoena or a search warrant. Govt C §7470(a)(1)-(4). See Govt C §§7471-7476. "Financial institution" for these purposes refers to both state and national banks, savings and loan associations, trust companies, and credit unions. Govt C §7465(a). A series of exceptions to the Act is set forth in Govt C §7480.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/9 Privacy Law and Privacy Policies/ e. Required Notice of Security Breaches/§9.24 (1) Civil Code Provisions

e. Required Notice of Security Breaches

§9.24 (1) Civil Code Provisions

California law requires companies and state agencies to inform California residents of any security breaches resulting in the theft of their personal information. See CC §§1798.29, 1798.82-1798.84. It requires a company to give the consumer notice if an unauthorized person has acquired the consumer's name and either Social Security number, driver's license number, financial account number, medical information, or health insurance information. See CC §1798.82(e).

NOTE: This law, which attracted attention as one of the first laws of its kind, has drawn criticism for failing to describe with specificity the actions companies must take to comply with the law. Nevertheless, experts have recognized that but for this California law, the ChoicePoint data security breach (see §9.9A) might never have come to light. In 2006, 13 states enacted legislation requiring companies or state agencies to disclose security breaches involving personal consumer information, bringing to at least 34 the total number of states with such laws. See http://www.ncsl.org/programs/lis/cip/priv/breach.htm. See also http://www.uspirg.org/financial-privacy-security/identity-theft-protection/summary-of-state-laws.

The law applies to companies based in California, as well as to any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information." CC §1798.82(a). At a minimum, companies are required to maintain technology for monitoring and identifying security breaches and to implement procedures for responding to and disclosing security breaches in accordance with the law.

Notice of a security breach may be provided by written notice, electronic notice complying with E-Sign (see §§7.5-7.8), or in some circumstances "substitute notice," which requires a combination of e-mail notice, conspicuous website posting, and notice to "major statewide media." CC §1798.82(g). Substitute notice may be used when the cost of notice will exceed $250,000, or when the number of persons to be notified exceeds 500,000, or when any person or business to be contacted does not have "sufficient contact information." CC §1798.82(g)(3).

See also the discussion of CC §§1798.82-1798.84 in §18.16.

NOTE: In a total of 44 states, plus the District of Columbia, Puerto Rico, and the U.S. Virgin Islands, notification laws are either currently in effect or scheduled to take effect in the future. States without breach notification laws at this time are Alabama, Kentucky, Mississippi, New Mexico, and South Dakota. However, practitioners should monitor this situation on state and federal levels.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/9 Privacy Law and Privacy Policies/§9.25 (2) Potential Safe Harbor

§9.25 (2) Potential Safe Harbor

One potential safe harbor exists under the statutes relating to a company's duty to notify a consumer of a security breach. Because the law defines "personal information" as "an individual's first name or first initial and last name *in combination with*" certain data elements such as a social security number, a driver's license number, a credit card number, health information, or health insurance information (emphasis added) (see CC §1798.82(e)), storing customer names separately from the other types of data identified in the statute might enable a company or an agency to avoid the disclosure obligations of the law.

The legislature further extended consumer privacy protection by enacting CC §1798.81.5, which requires businesses to implement reasonable procedures to maintain the security of personal information the business stores or discloses to third parties. See also the discussion of CC §§1798.82-1798.84 in §18.16.

PRACTICE TIP: The California Office of Privacy Protection has released "Recommended Practices on Notice of Security Breach Involving Personal Information" covering protection and prevention as well as procedures for data security breach notifications, sample forms, and letters. See http://www.privacy.ca.gov/res/docs/pdf/COPP_Breach_Reco_Practices_6-09.pdf. Although these recommended practices are not binding regulations, they provide valuable insights into the direction California law may take in the future and may serve as a reference point for courts reviewing the reasonableness of a business entity's practices and procedures.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/9 Privacy Law and Privacy Policies/§9.26 f. Civil Code §1798.83

§9.26 f. Civil Code §1798.83

Civil Code §1798.83 requires any business that has disclosed personal information in specified categories to third parties for direct marketing purposes to provide, on request, to customers with which the business has an "established business relationship," a list of the categories of information disclosed and the names and addresses of all third parties to whom the information has been disclosed. CC §1798.83(a). To facilitate disclosure requests from customers, businesses are required to take *one* of the following actions (CC §1798.83(b)):

- Notify all supervisors of employees with regular contact with customers to instruct those employees to give the business's contact information to customers requesting information about the business's privacy practices or compliance with CC §1798.83.
- Add a link titled "Your Privacy Rights" to the business's home page, or the words "Your Privacy Rights" to the home page's link to the business's privacy policy. The first page of the link must describe customers' rights under CC §1798.83 and provide contact information.
- Make contact information available to customers at every place where the company does business in California.

As an alternative way for a business to comply with CC §1798.83(a), a business may include in its privacy policy (see §§9.38-9.45) a policy of not disclosing customers' personal information to third parties for direct marketing purposes (1) unless the customer affirmatively consents to the disclosure, or (2) if the customer has exercised an "opt-out" mechanism. CC §1798.83(c)(2).

The statute lists certain disclosures of personal information that are not deemed to be disclosures of personal information to third parties for direct marketing purposes. See CC §1798.83(d). The statute also include a helpful, nonexclusive list of items that constitute "personal information" (CC §1798.83(e)(7)):

- An individual's name and address.
- Electronic mail address.
- Age or date of birth.
- Names of children.
- Electronic mail or other addresses of children.
- Number of children.
- Age or gender of children.
- Height.
- Weight.
- Race.
- Religion.
- Occupation.
- Telephone number.
- Education.
- Political party affiliation.
- Medical condition.
- Drugs, therapies, or medical products or equipment used.
- Kind of product the customer purchased, leased, or rented.
- Real property purchased, leased, or rented.
- Kind of service provided.
- Social security number.
- Bank account number.
- Credit card number.
- Debit card number.
- Bank or investment account, debit card, or credit card balance.

- Payment history.
- Information pertaining to the customer's creditworthiness, assets, income, or liabilities.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/9 Privacy Law and Privacy Policies/§9.26A g. California Protection Against Computer Spyware Act (Bus & P C §§22947-22947.6)

§9.26A g. California Protection Against Computer Spyware Act (Bus & P C §§22947-22947.6)

The Consumer Protection Against Computer Spyware Act (Bus & P C §§22947-22947.6) is intended to control spyware. It prohibits surreptitious installation of certain kinds of software on personal computers of California residents. The Act does not specifically define "spyware"; rather, it prohibits anyone who is not an "authorized user" from knowingly or willfully causing software to be copied onto the computer of a California resident when that software deceptively (Bus & P C §§22947.2-22947.3):

- Modifies certain settings related to the computer's Internet access or use (including changes to the computer's home page or any of the computer's bookmarks);
- Collects certain personally identifiable information identified in the Act;
- Prevents the user's reasonable efforts to block installation of the software or to disable the software, or intentionally misrepresents that an action will uninstall or disable the software, when the software will not be so uninstalled or disabled;
- Removes, disables, or renders inoperable any security, antispyware, or antivirus software on the computer;
- Takes control of the computer in order to transmit or relay commercial e-mail or a virus from that computer without authorization of the computer's authorized user;
- Uses the computer for the purpose of causing damage to another computer, such as by launching a "denial of service" attack; or
- Opens multiple, sequential, stand-alone advertisements (or "pop-ups") in the computer's Internet browser without authorization and "with knowledge that a reasonable computer user cannot close the advertisements" without closing the browser or shutting off the computer.

To be an "authorized user," a person or entity must either own the subject computer or be authorized by the owner or lessee to use the computer, provided, however, that it is not sufficient for that person or entity to obtain authorization solely from an end-user license agreement. Bus & P C §22947.1(b).

To protect legitimate monitoring and software installation activities, the Act includes a lengthy carve-out to allow "monitoring of, or interaction with," Internet connections or services by any (Bus & P C §22947.3(d)):

> telecommunications carrier, cable operator, computer hardware or software provider, or provider of information service or interactive computer service for network or computer security purposes, diagnostics, technical support, repair, authorized updates of software or system firmware, authorized remote system management, or detection or prevention of the unauthorized use of or fraudulent or other illegal activities in connection with a network, service, or computer software, including scanning for and removing software.

Section 22947.4, which prohibits the deceptive installation, copying, or execution of any software that is misrepresented as necessary for security purposes or is otherwise prohibited under the Act, contains a similar carve-out for these legitimate monitoring and interaction purposes. Bus & P C §22947.4.

NOTE: A number of antispyware efforts have come under criticism from mainstream technology businesses, particularly ISPs and security software developers, for the failure of these efforts to adequately define "spyware" so as to exclude legitimate (and sometimes essential) software provided by these companies. Counsel should encourage businesses that deliver software online via downloads to review the antispyware laws closely, to ensure that software delivery does not run afoul of any broadly drafted restrictions on such delivery.

© The Regents of the University of California

§9.27 h. Unfair Competition Law

California's unfair competition law, Bus & P C §§17200-17210, provides remedies for a wide range of unfair business practices, including, potentially, misrepresentation by a company of its privacy or data collection practices. The statute defines "unfair competition" as "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Bus & P C §17200.

Violations of the Consumer Protection Against Computer Spyware Act (Bus & P C §§22947-22947.6) are enforceable against companies as an act of unfair competition. See Analysis of Assembly Committee on SB 1436, available at http://info.sen.ca.gov/pub/03-04/bill/sen/sb_1401-1450/sb_1436_cfa_20040812_101755_asm_comm.html.

For an extensive discussion of California's unfair competition law, see California Business Litigation, chap 3 (Cal CEB 2002).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/9 Privacy Law and Privacy Policies/§9.27A D. Other States' Data Protection Programs

§9.27A D. Other States' Data Protection Programs

Many states outside California have adopted data security regulations requiring Internet companies to comply with a potentially confusing patchwork of laws. For example, Massachusetts and Nevada have both adopted data security requirements requiring encryption of data files containing personal information. The Nevada law provides that (Nev Rev Stats §597.970)

> [a] business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission.

The Massachusetts law requires encryption if the data will be transmitted wirelessly or across public networks or if the data will be stored on laptops or other portable devices. Mass Gen Laws ch 93H. The regulations implementing the Massachusetts law are very detailed and impose specific technical requirements on those who maintain personally identifiable data about state residents. See 201 Code Mass Regs §17.04. The compliance deadline for the Massachusetts law was March 1, 2010. 201 Code Mass Regs §17.05.

© The Regents of the University of California

§9.28 E. Special Legal Protections for Children

Most efforts in the United States to regulate Internet content and online user behavior to date have focused on children. Public concern for the online safety and privacy of children has resulted in several important initiatives, including in particular the Children's Online Privacy Protection Act of 1998 (COPPA) (15 USC §§6501-6506) (see §§9.29-9.34) as well as others (see §§9.35-9.36).

© The Regents of the University of California

§9.29 1. Children's Online Privacy Protection Act (COPPA)

The Children's Online Privacy Protection Act of 1998 (COPPA) (15 USC §§6501-6506) requires that website operators obtain parental consent before collecting "personal information" (see §9.31) from any child. The law defines "child" as anyone under the age of 13. 15 USC §6501(1). COPPA also specifies the ways in which consent must be obtained from parents and legal guardians. It includes only limited exceptions to the consent requirement.

The FTC enforces COPPA and, to implement it, has promulgated the Children's Online Privacy Protection Rule (16 CFR §§312.1-312.12). The Rule details requirements for privacy policies and parental notification by websites that are directed at children or that knowingly collect personal information from children. The Rule requires that each website or online service covered by its provisions have a privacy policy, and that a link to the policy "be placed in a clear and prominent place and manner on the home page of the website or online service," as well as in any area where children are asked to provide personal information. 16 CFR §312.4(b).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/9 Privacy Law and Privacy Policies/§9.30 a. Application of COPPA

§9.30 a. Application of COPPA

COPPA does not apply to all websites or online services. It applies only to operators of commercial websites and online services that are "targeted to children," as well as to any commercial website or online service operator "that has actual knowledge that it is collecting personal information from a child." 15 USC §6502(a). For websites or services that only partially target children, COPPA governs only the portion that targets children. 15 USC §6501(10)(A)(ii). For operators to which COPPA applies, personal information collected from children must be collected in accordance with COPPA requirements.

PRACTICE TIP: For many online businesses, the best way to avoid a COPPA violation is simply not to collect any personal information from children under the age of 13. Clients should be encouraged to consider this approach before undertaking an extensive program for COPPA compliance.

Whether a site is "targeted to children" can be determined by reference to extensive standards set out in the Rule (16 CFR §§312.1-312.12), including factors such as a website's subject matter, language, whether it uses animated characters, and whether advertising appearing on the site is directed to children. The FTC apparently will also consider empirical evidence regarding the ages of visitors to the site. The standards are intended to be similar to those previously established for television, radio, and print advertising. See Federal Trade Commission, Frequently Asked Questions About the Children's Online Privacy Protection Rule, Volume 1, available at http://www.ftc.gov/privacy/coppafaqs.htm.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/9 Privacy Law and Privacy Policies/§9.31 b. Requirements for Online Collection of Information From Children

§9.31 b. Requirements for Online Collection of Information From Children

COPPA applies only to personal information collected from children. It defines "personal information" as "individually identifiable information about an individual collected online," including a first and last name, a home address, an e-mail address, a telephone number, and a social security number, as well as any other information that "permits the physical or online contacting of a specific individual." 15 USC §6501(8). Personal information also includes any information collected online concerning a child or the parents of that child that is then combined with any of the foregoing identifiers. 15 USC §6501(8)(G).

If a website or online services operator desires to collect personal information from a child, the operator must (see 15 USC §6502(b); 16 CFR §§312.1-312.12):

- Post a COPPA-compliant privacy policy on its website;
- Provide notice to parents and, except in certain limited cases (see §9.32), obtain "verifiable parental consent" to the collection of personal information;
- Give parents certain choices with respect to the collection and use of their child's information, as well as the ability to review their child's information and ask to have it deleted; and
- Protect the confidentiality, security, and integrity of personal information collected from children.

PRACTICE TIP: Compliance with COPPA requires more from a company than just having in place a detailed privacy policy—it also requires a client's commitment to implement notification, confirmation, data collection, and security practices well beyond those required for other websites. Without a willingness to undertake such a commitment or without a business model that supports the additional administrative requirements and attendant expenses, clients should be counseled to avoid collecting information from children and avoid any website content that might be deemed to target children.

© The Regents of the University of California

§9.32 c. Parental Consent

The Children's Online Privacy Protection Rule (16 CFR §§312.1-312.12) addresses the question of what qualifies as "verifiable parental consent" and the kinds of consent that are required for COPPA compliance in different circumstances. See generally 16 CFR §312.5. It permits a tiered or "sliding scale" approach to parental consent:

- At the lower end of the scale, as long as an operator is not making further disclosure of a child's personal information to third parties, a parent may give consent by e-mail, provided that the e-mail consent is "coupled with additional steps to provide assurances that the person providing the consent is the parent." 16 CFR §312.5(b). Such additional steps may include a confirmatory e-mail sent to the parent after receipt of the consent or confirmation by telephone call or postal mail to a number or address obtained from the parent. When these follow-up methods are used, the follow-up should include notice that the parent can revoke any consent given in response to the initial e-mail. 16 CFR §312.5(b)(2).
- At the upper end of the scale, if a website operator plans to disclose to third parties personal information that it collects from children, the requirements for verifiable consent are far stricter, and include providing a consent form to be signed by the parent and returned to the operator by postal mail or facsimile; requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free telephone number staffed by trained personnel; using a digital certificate that uses public key technology; and using e-mail accompanied by a PIN or password obtained through one of the verification methods listed above. 16 CFR §312.5(b)(2).

On March 8, 2006, the FTC announced that it will retain the Children's Online Privacy Protection Rule, including the sliding scale mechanism, "indefinitely while it continues to monitor technological developments." See *FTC Retains Children's Online Privacy Protection (COPPA) Rule Without Changes* (Mar. 8, 2006), available at http://www.ftc.gov/opa/2006/03/coppa_frn.htm. In the report accompanying this decision, the FTC stopped short of adopting the Rule as permanent, in case future technological developments warranted its re-evaluation, but did not indicate that there would be any changes to the Rule in the near term. See http://www.ftc.gov/os/2006/03/P054505COPPARuleRetention.pdf.

© The Regents of the University of California

§9.33 d. Enforcement

Under COPPA, the FTC can bring a civil enforcement action for a cease-and-desist order or a monetary penalty against a website operator for any failure to comply with COPPA or the Children's Online Privacy Protection Rule. Each instance of unlawful or unauthorized collection, use, or disclosure of a child's personal information is counted as a separate violation of the Act, so the potential monetary liability is not insignificant—up to $11,000 per violation. 15 USC §45(m)(1)(A) ($10,000 per violation, plus upward adjustment for inflation). Monetary penalties have been significant elements in FTC settlements of recent COPPA cases: In two settlements announced in February 2003, Mrs. Fields Cookies and Hershey Foods Corporation agreed to pay $100,000 and $85,000, respectively, for alleged violations of COPPA. See FTC Consent Decree and Order, *U.S. v Hershey Foods* (Mar. 6, 2003, Civ. Action No. 4:CV03-350), available at http://www.ftc.gov/os/2003/02/hersheyconsent.htm; FTC Consent Decree and Order, *U.S. v Mrs. Fields Famous Brands, Inc.* (Mar. 6, 2003, Civ. Action No. CV205 JTG), available at http://www.ftc.gov/os/2003/02/mrsfieldsconsent.htm. In settlements announced in February 2004, UMG Recordings, Inc., and Bonzi Software, Inc., agreed to pay $400,000 and $75,000, respectively, for alleged violations of COPPA. See FTC Consent Decree and Order, *U.S. v UMG Recordings, Inc.* (Feb. 18, 2004, Civ Action No. CV-04-1050 JFW) (http://www.ftc.gov/os/caselist/umgrecordings/040217cagumgrecordings.pdf); and FTC Consent Decree and Order, *U.S. v Bonzi Software, Inc.* (Feb 18, 2004, Civ Action No. CV-04-1048 RJK) (http://www.ftc.gov/os/caselist/bonzi/040217decreebonzi.pdf). According to the FTC, the Bonzi Software action was the first case under COPPA to address information collection practices that an online service conducted through a software product; prior COPPA cases had been directed at the information collection practices of website operators. See *UMG Recordings, Inc. to Pay $400,000, Bonzi Software, Inc. To Pay $75,000 to Settle COPPA Civil Penalty Charges* at http://www.ftc.gov/opa/2004/02/bonziumg.htm.

In 2009 the FTC reached a settlement with Iconix Brand Group, Inc., an online apparel marketer, requiring payment of a $250,000 civil penalty and additional operational requirements, including annual compliance reporting to the FTC for the next 5 years and linking any Iconix website that collects personal information from users to the FTC's http://www.OnGuardOnline.gov website. As is typical in FTC actions of this type, Iconix was required to delete any children's information collected and maintained in violation of COPPA. See FTC Consent Decree and Order, *U.S. v Iconix Brand Group, Inc.* (Nov. 5, 2009, Civ Action No. 09 Civ 8864 (MGC) (http://www.ftc.gov/os/caselist/0923032/091020Iconixsonsentorder.pdf).

In September 2006, the FTC announced its largest penalty ever for a COPPA violation: $1 million, paid by online social networking site Xanga.com, Inc., and its two principals. The penalty was more than twice as large as the next largest penalty that the FTC had levied. *Xanga.com to Pay $1 Million for Violating Children's Online Privacy Protection Rule* (Sept. 7, 2006), available at http://www.ftc.gov/opa/2006/09/xanga.shtm. The FTC alleged that Xanga had collected, used, and disclosed personal information from children under the age of 13 without complying with COPPA. Over a period of 5 years, more than 1.7 million Xanga accounts were created by users who had provided a birth date indicating they were under the age of 13; Xanga failed to notify those users' parents of Xanga's information practices and failed to provide parents with the necessary access to and control over their children's information. In addition to the $1 million fine, the FTC's consent order required Xanga and its two principals to take steps to avoid further violations of COPPA. *U.S. v Xanga.com, Inc.* (Sept. 7, 2006, Civ Action No. 06-CIV-6853 SHS FTC File No. 062-3073), available at http://www.ftc.gov/os/caselist/0623073/index.htm.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/9 Privacy Law and Privacy Policies/§9.34 e. Safe Harbor

§9.34 e. Safe Harbor

In a few circumstances under COPPA, parental consent is not required at all for collection of personal information from children. A website operator need not obtain the parental consent otherwise required by COPPA:

- If the website collects online contact information from a child in order to respond, on a one-time basis only, to a specific request from that child, and the website does not re-contact the child or store the contact information in any retrievable form. 15 USC §6502(b)(2)(A). See also 15 USC §6502(b)(2)(C).
- If the website requests a name or the online contact information for a parent or child, uses that information for the sole purpose of obtaining parental consent or providing notice under COPPA, and does not store the contact information in any retrievable form if parental consent has not been obtained after a reasonable time. 15 USC §6502(b)(2)(B).
- If the website collects online contact information from a child in order to respond, more than once, to a specific request from that child, and the website does not re-contact the child beyond the scope of that request, provided that:
- After the first response and before any additional response, the website makes reasonable efforts to give a parent of the child notice of the information collected, the purpose for which it is to be used, and an opportunity for the parent to request that the website make no further use of the information and not store it in any retrievable form; or
- Without notice to a parent of the child, if provided by FTC regulations. 15 USC §6502(b)(2)(C).
- If the website obtains a child's name and contact information to the extent reasonably necessary in order to protect the safety of a child participant on the website, as long as:
- The name and contact information are only used to protect such child's safety, and not used or disclosed for any other purposes; and
- The website operator takes reasonable steps to provide a parent of the child with notice of the information collected from the child and the purposes for which it will used, and provides the parent with an opportunity to request that no further use be made of the information and that it not be maintained in retrievable form. 15 USC §6502(b)(2)(D).
- If the collection, use, or dissemination of any child's personal information is necessary to protect the security or integrity of the website, to take precautions against liability, or to respond to judicial process or other legal requirements. 15 USC §6502(b)(2)(E).

© The Regents of the University of California

§9.35 2. Dot-Kids Act

The Dot-Kids Implementation and Efficiency Act of 2002 (Dot-Kids Act) (Pub L 107-317, 116 Stat 2766) created a "kid-safe" area known as "Dot-Kids" located at kids.us and overseen by the federal government. The plan for kids.us is to ensure that all included material is appropriate for children under the age of 13. Content to be included on kids.us websites must be submitted for approval before website activation, and registrars who wish to sell domain names in the kids.us domain must meet certain requirements set out in the Dot-Kids Act. Additional information on dot-kids implementation and registration is available at http://www.kids.us.

© The Regents of the University of California

§9.36 3. Kidz Privacy Website

The FTC has mounted an educational campaign that targets parents, children, businesses, and the media in an effort to promote safe Internet use by children and to assist interested parties in understanding their rights and responsibilities under COPPA (see §§9.29-9.34). The FTC has dedicated a portion of its website to this effort. The FTC website offers information on children's privacy for parents at http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec08.shtm. Information for teachers is available at http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec10.shtm. The FTC permits parents and others to submit privacy complaints to the FTC website at http://www.ftc.gov and through a toll-free telephone number.

© The Regents of the University of California

F. European Privacy Directive

§9.37 1. Scope of Directive

Although Internet privacy regulation in the United States has largely consisted of industry self-regulation, Europe and other parts of the world have enacted substantive legislation or other express policies. In 1995, the European Union adopted the Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, also known as the EU Privacy Directive. See EU Directive No. 95/46/EC (Oct. 24, 1995), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

The EU Privacy Directive specifies that "data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent." EU Directive No. 95/46/EC (Oct. 24, 1995), Recitals (33). European Union member states must ensure that personal data are (EU Directive No. 95/46/EC (Oct. 24, 1995), art 6):

- Processed fairly and lawfully;
- Collected for specified, explicit, and legitimate purposes, and not further processed in a manner incompatible with those purposes;
- Adequate, relevant, and not excessive with respect to the purposes;
- Accurate and kept up to date; and
- Kept in a form that permits identification of the consumer for no longer than necessary.

NOTE: The EU Privacy Directive applies to individuals and not legal entities. However, because it may affect employees, it may thus impact the way electronic commerce is conducted, particularly with respect to multinational companies. The Privacy Directive also applies to the way information about customers may be collected from websites, the way it may be transferred, and how it may be used. See Ballon, E-Commerce and Internet Law §32.04[1][A] (2001).

In 1997 and 2002, the European Union adopted directives specifically related to privacy in electronic communications and telecommunications. See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML. In 2006, the European Union adopted a directive aimed at harmonizing the laws of its member states concerning the retention of communications traffic and location data (as distinguished from the actual contents of the communications) by providers of publicly available electronic communications services and public communications networks. A stated goal of the directive was "to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law." EU Directive No. 2006/24/EC (Mar. 15, 2006), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

© The Regents of the University of California

§9.38 2. Safe Harbor

The EU Privacy Directive provides that, without the consumer's consent, personal data may not be transferred to a third country outside of the EU (*e.g.,* the United States) unless the third country ensures "an adequate level of protection." Directive No. 95/46/EC (Oct. 24, 1995), art 25(1). This provision of the EU Privacy Directive might have represented an obstacle to commerce between the United States and EU members, but the United States Department of Commerce and the European Commission negotiated a compromise known as the Safe Harbor Accord. Provisions of the Accord, as well as methods to assist companies in taking advantage of it, are available at http://www.export.gov/safeharbor.

To comply with the Accord, a company must comply with a set of privacy principles issued by the U.S. Department of Commerce. The EU has indicated that a company following these principles will satisfy the "adequate level of protection" requirement of the EU Privacy Directive. See U.S. Department of Commerce, Commission Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbor Privacy Principles and Frequently Asked Questions, available at http://www.ita.doc.gov/td/ecom/DecisionSECGEN-EN.htm.

PRACTICE TIP: To learn how to comply with the Safe Harbor Accord, a company should consult the Frequently Asked Questions (FAQs) available on the U.S. Department of Commerce's website. See http://www.export.gov/safeharbor.

© The Regents of the University of California

III. WEBSITE PRIVACY POLICIES

§9.39 A. Need for Privacy Policies

Commercial website operators and online services that serve California consumers are legally obligated to develop and post privacy policies on their websites. Bus & P C §22575(a). For a discussion of the California Online Privacy Protection Act of 2003 (Bus & P C §§22575-22579), see §§9.19-9.21.

The basic purpose of a privacy policy is disclosure. Consumers may tolerate a wide variety of uses of their personal information without objection as long as they are informed about those uses in advance. Disputes over privacy issues are often a result of incomplete or inadequate disclosures relating to a website's use of consumer information. For example, after online advertiser DoubleClick announced its December 1999 merger with Abacus Direct, an offline company that maintained databases on catalog customers, there was public outcry over the privacy implications of the merger. See, *e.g.,* Masterson, "DoubleClick in New Suit," money.cnn.com, Feb. 17, 2000, available at http://money.cnn.com/2000/02/17/technology/doubleclick. Privacy advocates and watchdog organizations sought to prevent DoubleClick from combining its previously anonymous consumer database with Abacus Direct's database of information about catalog shoppers; the proposed combination would create an enormous database of the online and offline shopping and spending habits of millions of identifiable consumers, allegedly in breach of promises regarding anonymity of data that DoubleClick had previously made in privacy policies in effect prior to the Abacus merger. Ultimately, the negative publicity led DoubleClick to abandon any plans to combine the databases after the merger. No governmental enforcement action was taken (the FTC closed its investigation into the matter without taking any further action; see http://www.ftc.gov/os/closings/staff/doubleclick.pdf), but this case served as an impetus for privacy regulation.

© The Regents of the University of California

§9.40 B. Content of Privacy Policies

No single form of privacy policy will meet the needs of every company doing business online. A good privacy policy must be specifically tailored to a company's requirements. Input from counsel is crucial to help the client draft and implement a policy that complies with applicable law and accurately reflects the client's business and data collection practices.

Preparation of an appropriate website privacy policy begins with a thorough understanding of the client's business and its website data collection practices, as well as the sources of personal information collected. Issues relating to children should be addressed with reference to the Children's Online Privacy Protection Act of 1998 (COPPA) (15 USC §§6501-6506) (see §§9.29-9.34), which may require that the business adopt additional procedures for notice, consent, security, and confidentiality. Issues concerning transfer of data from European countries should be addressed with respect to the EU Privacy Directive and the resulting Safe Harbor Accord. See §§9.37-9.38. The forms of website privacy policies in §§9.44 and 9.46 should serve as starting points for drafting. Counsel should review the key aspects of a client's information-gathering practices and tailor the forms to reflect those practices, adding additional terms as needed for clients with more complex websites.

The terms and conditions of a privacy policy represent promises to which a business will be held by its customers and by the FTC and should be treated like any other contract, with an understanding that breach of these terms could result in serious financial harm and damage to the business's reputation.

In addition to disclosure issues, company privacy practices usually involve decisions regarding the extent of consumer choices allowed. Customers are often asked to choose whether and to what extent information about them will be collected. At the most privacy-favorable level, customers are given a choice to have no information about them at all—either anonymous or identifiable—collected. More often, however, websites are programmed to collect certain anonymous data (such as referring IP addresses and the number of site visitors; see §§9.4-9.5) automatically, and they do not give customers an option to prevent collection of this type of information. In e-commerce transactions, collection of personal information is normally required for payment and order fulfillment purposes, but disclosure of that information to third parties is often completely optional, with users given a choice whether to permit or prohibit such disclosure.

Thus, each website operator must decide how to let customers define their privacy choices. A website's approach to data collection and use can be either "opt-in," in which users expressly consent to have their personal information used in ways identified by the website operator, or "opt-out," in which the website operator will use personal information in the ways described in its privacy policy unless a user specifically requests that his or her information not be so used. For users who have either opted in or not elected to opt out (depending on how the website is configured), the privacy policy should disclose, as completely and clearly as possible, the ways in which collected information is used and the extent to which that information will be shared with third parties. The form privacy policies reproduced in §§9.44 and 9.46 suggest ways in which these disclosures might be made.

© The Regents of the University of California

§9.41 C. Enforceability of Privacy Policies

Because website privacy policies are a type of online agreement between a company and users of its website, counsel should give thought to the enforceability of the policy and the manner (if any) in which users are asked to accept its terms. Often, a privacy policy is simply made available by a link at the bottom of the home page, and users are never specifically requested to accept the policy in order to access or use the website. This absence of specific acceptance may create enforceability problems, at least for privacy policy terms that fall outside the ambit of FTC enforcement. For a detailed discussion of enforceability issues concerning online agreements, see chap 7. See also the California requirements for posting privacy policies in Bus & P C §22577(b)(1)-(5), discussed in §9.19.

© The Regents of the University of California

§9.42 D. Additional Resources

Many online resources are available for preparation of website privacy policies. Chief among them is the FTC, which devotes a large section of its website to privacy initiatives. See, *e.g.,* http://www.ftc.gov/privacy. In addition, privacy watchdogs such as the Electronic Frontier Foundation (http://www.eff.org) and the Electronic Privacy Information Center (http://www.epic.org) offer privacy resources and tools to assist consumers and businesses stay up to date on privacy regulation and understand their rights and obligations under privacy laws. Finally, businesses should consider obtaining certification from a nonprofit privacy organization such as TRUSTe (http://www.truste.org), which operates a voluntary "privacy seal" program designed to inform users that a website operator has committed to meet certain standards in collection and handling of user information.

© The Regents of the University of California

E. Basic Website Policy

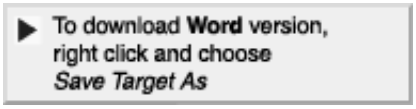
§9.43 1. Introduction

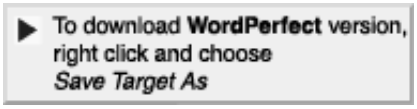
The form in §9.44 is a basic form of website privacy policy statement, designed to meet the needs of website sponsors that do not wish to undertake a substantial administrative burden to manage customer information. For example, the policy requires that all website users permit data collection as a condition of their use of the website, and except for third party offers, does not include any language indicating that users can elect whether or not to have their personal information collected or to designate how that information may be used. The policy form is intended to conform with the requirements of the California Online Privacy Protection Act of 2003 (Bus & P C §§22575-22579). See §§9.19-9.21.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/9 Privacy Law and Privacy Policies/§9.44 2. Form: Basic Website Privacy Policy

§9.44 2. Form: Basic Website Privacy Policy





WEBSITE PRIVACY POLICY
EFFECTIVE DATE: _ _[*Date*]**_ _**

1. INTRODUCTION

1.1. PURPOSE OF POLICY. _ _[*Name of website operator*]**_ _ ("us," "we," or "Company") is committed to respecting the privacy rights of its customers, visitors, and other users of the Company Website (the "Site"). We created this Website Privacy Policy (this "Policy") to give you confidence as you visit and use the Site, and to demonstrate our commitment to fair information practices and the protection of privacy. This Policy is only applicable to the Site, and not to any other websites that you may be able to access from the Site, each of which may have data collection and use practices and policies that differ materially from this Policy.**

1.2. NOTICE CONCERNING CHILDREN

PLEASE NOTE: We are a general audience site, and do not direct any of our content specifically at children under 13 years of age. We understand and are committed to respecting the sensitive nature of children's privacy online. If we learn or have reason to suspect that a Site user is under age 13, we will promptly delete any personal information in that user's account.

2. INFORMATION COLLECTION PRACTICES

2.1. WHAT BASIC INFORMATION DOES THE COMPANY COLLECT?

In operating the Site, Company may include registration, online surveys, and other online forms that ask users to provide their names, e-mail addresses, and other contact information, as well as the following categories of information: _ _[*identify categories of information to be collected*]**_ _.**

2.2. WHAT ADDITIONAL INFORMATION DOES COMPANY COLLECT?

(a) AUTOMATIC COLLECTION. Our servers automatically recognize visitors' domain names and IP addresses (the number assigned to computers on the Internet). No personal information about you is revealed in this process. The Site may also gather anonymous "traffic data" that does not personally identify you, but that may be helpful for marketing purposes or for improving the services we offer.

(b) COOKIES. From time to time, we may use the standard "cookies" feature of major browser applications that allows us to store a small piece of data on your computer about your visit to our Web site. We do not set any personally identifiable information in cookies, nor do we employ any data capture mechanisms on our website other than cookies. Cookies help us learn which areas of our site are useful and which areas need improvement. You can choose whether to accept cookies by changing the settings on your browser. However, if you choose to disable this function, your experience at our Web site may be diminished and some features may not work as they were intended.

3. USE AND SHARING OF INFORMATION

3.1. WHAT DOES COMPANY DO WITH COLLECTED INFORMATION?

(a) PERSONAL INFORMATION. We will not share your personal information with any third parties without your consent, except as necessary to provide you with the services offered by us or to comply with the law. We may use your personal information to verify your identity, to check your qualifications, or to follow up with transactions initiated on the Site. We may also use your contact information to inform you of any changes to

the Site, or to send you additional information about Company. If you give your permission during the account registration process, we may share your contact information with our business partners or other companies so that they may send you promotional materials.

(b) ANONYMOUS INFORMATION. We use anonymous information to analyze our Site traffic, but we do not examine this information for individually identifying information. In addition, we may use anonymous IP addresses to help diagnose problems with our server, to administer our site, or to display the content according to your preferences. Traffic and transaction information may also be shared with business partners and advertisers on an aggregate and anonymous basis.

(c) USE OF COOKIES. We may use cookies to deliver content specific to your interests, to save your password so you don't have to re-enter it each time you visit our site, or for other purposes. Promotions or advertisements displayed on our site may contain cookies. We do not have access to or control over information collected by outside advertisers on our site.

(d) DISCLOSURE OF PERSONAL INFORMATION. We may disclose personal information if required to do so by law or in the good-faith belief that such action is necessary to (1) conform to the edicts of the law or comply with legal process served on Company or its parent company, subsidiaries or affiliates, (2) protect and defend the rights or property of Company or the users of the Site, or (3) act under exigent circumstances to protect the safety of the public or users of the Site.

(e) SALE OF INFORMATION. In order to accommodate changes in our business, we may sell or buy portions of our company or other companies or assets, including the information collected through this Web site. If Company or substantially all of its assets are acquired, customer information will be one of the assets transferred to the acquirer.

(f) ACCESS TO INFORMATION. Unfortunately, we do not maintain any procedures for you to review or request changes to the information that we collect about you, except that you may request that we remove all information about you from our database by contacting us in accordance with Section 6.1 below.

4. SECURITY

The Site has security measures in place to prevent the loss, misuse, and alteration of the information that we obtain from you, but we make no assurances about our ability to prevent any such loss, misuse, to you or to any third party arising out of any such loss, misuse, or alteration.

5. WEBSITE AREAS BEYOND COMPANY'S CONTROL

5.1. PUBLIC FORUMS

The Site may include interactive forums such as message boards and chat rooms. Please remember that any information that is disclosed in these areas becomes public information and you should exercise caution when deciding to disclose your personal information.

5.2. THIRD PARTY WEBSITES

The Site may contain links to other websites. If you choose to visit other websites, we are not responsible for the privacy practices or content of those other websites, and it is your responsibility to review the privacy policies at those websites to confirm that you understand and agree with their policies.

6. CONTACT INFORMATION AND POLICY UPDATES

6.1. CONTACTING US

If you have any questions about this Policy, our practices related to this Site, or if you would like to have us remove your information from our database please feel contact us at the following _ _[*e-mail address/telephone number/address*]_ _:

_ _[*Contact information*]_ _

6.2. UPDATES AND CHANGES

We reserve the right, at any time, to add to, change, update, or modify this Policy, simply by posting such change, update, or modification on the Site and without any other notice to you. Any such change, update, or modification will be effective immediately upon posting on the Site. It is your responsibility to review this Policy from time to time to ensure that you continue to agree with all of its terms.

© The Regents of the University of California

F. Commercial Website Policy

§9.45 1. Introduction

For some online businesses, the collection, storage, and use—and often disclosure to third parties—of personal customer information is a necessary part of the business model. For example, an e-commerce website could not operate successfully without being able to collect personal financial information from customers and share that information with business partners responsible for core business functions such as billing or order fulfillment. For e-commerce sites, comprehensive privacy policies are required. The form in §9.46, which reflects a survey of privacy terms that might be advisable, should not be used without extensive consideration of a client's particular needs for data collection, storage, and use, as well as the client's ability to accommodate a range of customer requests for handling personal information—from no storage or disclosure at all, to storage, use, and disclosure sufficient to serve all of the needs of the company and its partners. The policy form is intended to conform with the requirements of the California Online Privacy Protection Act of 2003 (Bus & P C §§22575-22579). See §§9.19-9.21.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/9 Privacy Law and Privacy Policies/§9.46 2. Form: Commercial Website Privacy Policy

§9.46 2. Form: Commercial Website Privacy Policy

▶ To download **Word** version, right click and choose *Save Target As*

▶ To download **WordPerfect** version, right click and choose *Save Target As*

WEBSITE PRIVACY POLICY
EFFECTIVE DATE: _ _[*Date*]_ _

1. INTRODUCTION. _ _[*Name of website operator*]_ _("us," "we," or "Company") is committed to respecting the privacy rights of its customers, visitors, and other users of the Company Website ("the Site"). We created this Website Privacy Policy ("Privacy Policy") to give you confidence as you visit and use the Site, and to demonstrate our commitment to fair information practices and the protection of privacy. This Privacy Policy is only applicable to the Site, and not to any other websites that you may be able to access from the Site, each of which may have data collection, storage, and use practices and policies that differ materially from this Privacy Policy.

2. INFORMATION COLLECTION PRACTICES

2.1. TYPES OF INFORMATION COLLECTED

(a) TRAFFIC DATA COLLECTED. We automatically track and collect the following categories of information when you visit our Site: (1) IP addresses; (2) domain servers; (3) types of computers accessing the Site; and (4) types of web browsers used to access the Site (collectively "Traffic Data"). Traffic Data is anonymous information that does not personally identify you but is helpful for marketing purposes or for improving your experience on the Site. We also use "cookies" to customize content specific to your interests, to ensure that you do not see the same advertisement repeatedly, and to store your password so you do not have to re-enter it each time you visit the Site.

(b) PERSONAL INFORMATION COLLECTED. In order for you to access certain premium, services and to purchase products that we offer via the Site, we require you to provide us with certain information that personally identifies you ("Personal Information"). Personal Information includes the following categories of information: (1) Contact Data (such as your name, mailing address, and e-mail address); (2) Financial Data (such as your account or credit card number); and (3) Demographic Data (such as your zip code, age, and income). If you communicate with us by e-mail, post messages to any of our chat groups, bulletin boards, or forums, or otherwise complete online forms, surveys, or contest entries, any information provided in such communication may be collected as Personal Information.

2.2. USES OF INFORMATION COLLECTED

(a) COMPANY USE OF INFORMATION. We use Contact Data to send you information about our company or our products or services, or promotional material from some of our partners, or to contact you when necessary. We use your Financial Data to verify your qualifications for certain products or services and to bill you for products and services. We use your Demographic Data to customize and tailor your experience on the Site, displaying content that we think you might be interested in and according to your preferences.

(b) SHARING OF PERSONAL INFORMATION. We share certain categories of information we collect from you in the ways described in this Privacy Policy. We share Demographic Data with advertisers and other third parties only on an aggregate (*i.e.,* non-personally-identifiable) basis. We share Contact Data with other companies who may want to send you information about their products or services, unless you have specifically requested that we not share Contact Data with such companies. We also share Contact Data and Financial Data with our business partners who assist us by performing core services (such as hosting, billing, fulfillment, or data storage and security) related to our operation of the Site. Those business partners have all agreed to uphold the same standards of security and confidentiality that we have promised to you in this Privacy Policy, and they will only use your Contact Data and other Personal Information to carry out their specific business obligations to Company. If you do not want us to share your Contact Data with any third

parties, please email us at _ _[*e-mail address of website operator*]_ _ or select the "opt out" box on our online forms, but please understand that such a request will likely limit your ability to take advantage of all of the features and services we offer on the Site. In addition, we maintain a procedure for you to review and request changes to your Personal Information; this procedure is described in Section 3.1, below.

(c) USER CHOICE REGARDING COLLECTION, USE, AND DISTRIBUTION OF PERSONAL INFORMATION. You may choose not to provide us with any Personal Information. In such an event, you can still access and use much of the Site; however you will not be able to access and use those portions of the Site that require your Personal Information. If you do not wish to receive information and promotional material from us or from some of our partners, you may select the appropriate "opt-out" option each time we ask you for Personal Information.

3. CONFIDENTIALITY AND SECURITY OF PERSONAL INFORMATION. Except as otherwise provided in this Privacy Policy, we will keep your Personal Information private and will not share it with third parties, unless such disclosure is necessary to: (a) comply with a court order or other legal process; (b) protect our rights or property; or (c) enforce our Terms of Service. Your Personal Information is stored on secure servers that are not accessible by third parties. We provide you with the capability to transmit you Personal Information via secured and encrypted channels if you use a similarly equipped web browser.

3.1. USER ABILITY TO ACCESS, UPDATE, AND CORRECT PERSONAL INFORMATION. We maintain a procedure in order to help you confirm that your Personal Information remains correct and up-to-date. At any time, you may visit your personal profile at _ _[*web address used by website operator for user access to Personal Information*]_ _. Through your personal profile you may: (a) review and update your Personal Information that we have already collected; (b) choose whether or not you wish us to send you information about our company, or promotional material from some of our partners; and/or (c) choose whether or not you wish for us to share your Personal Information with third parties.

3.2. LOST OR STOLEN INFORMATION. You must promptly notify us if your credit card, user name, or password is lost, stolen, or used without permission. In such an event, we will remove that credit card number, user name, or password from your account and update our records accordingly.

3.3. PUBLIC INFORMATION. The Site contains links to other websites. We are not responsible for the privacy practices or the content of such websites. We also make chat rooms, forums, message boards, and news groups available to you. Please understand that any information that is disclosed in these areas becomes public information. We have no control over its use and you should exercise caution when deciding to disclose your Personal Information.

4. UPDATES AND CHANGES TO PRIVACY POLICY. We reserve the right, at any time and without notice, to add to, change, update, or modify this Privacy Policy, simply by posting such change, update, or modification on the Site and without any other notice to you. Any such change, update, or modification will be effective immediately upon posting on the Site.

© The Regents of the University of California

10

E-Commerce Transactions and Tax Issues

I. E-COMMERCE TRANSACTIONS
- A. Introduction §10.1
- B. Electronic Contracting §10.2
- C. Forms of Payment
  - 1. Credit Cards §10.3
  - 2. Debit Cards §10.4
  - 3. Internet Checks §10.5
  - 4. Other Electronic Payment Services §10.6
- D. Additional Payment and Security Issues §10.7
  - 1. Secure Transaction Processing Software §10.8
  - 2. Fraud Prevention Tools §10.9
  - 3. Phone and Fax Orders §10.10
  - 4. Security Certificates §10.11
- E. Shopping Cart Services
  - 1. Overview §10.12
  - 2. Evaluating Shopping Cart Services §10.13
- F. Sample Website End User Payment Terms
  - 1. Introduction §10.14
  - 2. Form: Sample Clauses re Payment of Subscription Fees §10.15
- G. FTC's Mail or Telephone Order Merchandise Rule §10.16

II. TAX ISSUES
- A. Formulation of E-Commerce Tax Policy §10.17
  - 1. International Tax Policy §10.18
  - 2. United States Federal Tax Policy
    - a. Role of Treasury Department §10.19
    - b. The Internet Tax Freedom Act and Recent Developments §10.20
    - c. The Streamlined Sales Tax Agreement §10.20A
  - 3. California Tax Policy §10.21
- B. Sales and Use Taxes
  - 1. General Principles §10.22
  - 2. Constitutional Restrictions on Use Tax Collection Obligations §10.23
  - 3. California Sales and Use Taxes §10.24
  - 4. California Sales and Use Tax Treatment of Software Sales and Related Services §10.25

© The Regents of the University of California

I. E-COMMERCE TRANSACTIONS

§10.1 A. Introduction

The total dollar value of U.S. retail sales transactions over the Internet has been predicted to exceed $100 billion by the year 2010. Sections 10.2-10.16 explore some basic issues related to commercial sales transactions on the Internet. Online payment systems (including model payment provisions for a website's terms of use) and "shopping carts" are discussed in §§10.3-10.13. Sections 10.14-10.15 include sample clauses regarding subscription fee payment for a website terms of use. Section 10.16 discusses the Federal Trade Commission rule governing shipment and delivery of products sold. Finally, taxation of e-commerce transactions is discussed in §§10.17-10.25.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/10 E-Commerce Transactions and Tax Issues/§10.2 B. Electronic Contracting

§10.2 B. Electronic Contracting

E-commerce transactions, like most purchase and sale transactions regardless of format, involve documents containing the terms of sale and signatures of the parties indicating their assent to those terms, although the purchase and sale contract and signatures of the parties are in electronic form. Concerns as to whether electronic documents and signatures are enforceable have been addressed by federal and state legislation, including the Electronic Signatures in Global and National Commerce Act (E-Sign) (15 USC §§7001-7006, 7021, 7031, and 47 USC §231), and the Uniform Electronic Transactions Act (UETA) (see CC §§1633.1-1633.17). These measures are discussed in chap 7.

© The Regents of the University of California

C. Forms of Payment

§10.3 1. Credit Cards

For credit-card transactions on the Internet, customers enter credit card information into browser-based forms. The data is encrypted, captured by the transaction processor's secure payment gateway, and sent to credit card processing networks for authorization. Transactions normally settle in two to three business days. The merchant must have a relationship with a transaction processor in order to be able to receive credit card payments and pay credit card processing and transaction fees. Credit card payments are processed in one of two ways: batch processing or real-time processing. In batch processing, credit card payment orders are batched and submitted for processing at a given time each day. In real-time processing, credit card payment orders are processed and cleared at the same time that they are entered into the system. Higher fees are normally charged for real-time processing.

© The Regents of the University of California

§10.4 2. Debit Cards

There are two types of debit card transactions: online and offline. Online debit transactions are not presently conducted over the Internet, but rather over proprietary point-of-sale (POS) networks. Customers paying with debit cards in "brick-and-mortar" stores swipe their cards through magnetic card readers (POS terminals) and then enter their personal identification numbers (PINs) into the terminal. Debit card transactions are processed through POS terminals in real time through nationwide banking networks. Funds in customers' accounts are captured immediately and transferred to merchants' accounts in two to three business days. Merchants typically pay discount and transaction fees based on rates set by the networks. At present, no adequate operating protocols exist for processing PINs securely over the Internet. However, new industry initiatives are expected to advance the development of PIN-based debit programs for e-commerce transactions in the future.

Unlike online debit transactions, offline debit payments do not involve PINs. Offline debit cards (also called "check cards") are typically issued by large credit card companies through their participating banks. These enhanced ATM cards carry either Visa or MasterCard logos and may be used everywhere that credit cards are accepted, including over the Internet. Because check card transactions are processed through the same networks as credit cards, the same transaction fees are typically charged for processing. A merchant who already has credit card processing capability should be able to accept check cards without incurring additional fees.

© The Regents of the University of California

§10.5 3. Internet Checks

Some payment-processing software allows e-commerce website customers to have funds debited from their checking accounts. Customers key their checking account number and the amount of the payment into a browser-based form, and the data is encrypted and captured by the transaction processor's payment gateway. Funds from approved transactions are debited from customers' accounts and transferred through the automated clearing house (ACH) network into merchants' accounts in 10 to 14 days.

© The Regents of the University of California

§10.6 4. Other Electronic Payment Services

Other models for secure funds transfers and transaction payments over the Internet are rapidly developing. These include "digital cash," stored-value cards, online escrow services, and online payment systems such as PayPal or Western Union's BidPay. PayPal uses existing banking networks to enable any business or consumer with an e-mail address to send and receive payments online. BidPay enables customers to purchase Western Union money orders online and in turn transmits the money orders to online auction sellers by U.S. mail. These services are winning increasing acceptance by consumers, but credit cards remain the most popular method for processing e-commerce payments.

© The Regents of the University of California

§10.7 D. Additional Payment and Security Issues

To accept credit cards, an online merchant must contract with a credit card processing service. Most commercial banks can provide this service, and a merchant's long-term relationship with its own bank may offer advantages. Some banks specialize in issuing accounts to online merchants, but may charge higher up-front fees or higher fees for equipment rental or payment processing. Merchants should investigate the range of possible fees and how the fees may be affected by the volume of transactions. Sections 10.8-10.11 discuss additional issues related to processing credit card payments online.

© The Regents of the University of California

§10.8 1. Secure Transaction Processing Software

Electronic signatures are now legally enforceable (see §7.6), but there is a difference between an electronic signature that is legally sufficient and one that is trustworthy. Businesses operating on the Internet must have methods to ensure the identity of their customers and the integrity of online documentation for e-commerce transactions. There are various systems in use to authenticate a customer's identity.

Secure payment transaction software processes customer order information and verifies addresses, credit card numbers, and other customer data. This software can often be obtained as part of the credit card processing service offered by a financial institution or by a web hosting service, or it may be purchased directly from the software vendor. The software, also known as a gateway, sends the data to a secure credit card authorization network, which encrypts the data, verifies that the customer's credit card is valid, and verifies that the billing address given by the customer matches the billing address in the card issuer's records. Customers know that they have a secure server connection when the URL in their browser reads "https://"— the "s" stands for "secure." The secure payment gateway protects merchants and their customers by reducing the risk of fraud and preventing interception by computer hackers.

© The Regents of the University of California

§10.9 2. Fraud Prevention Tools

One fraud prevention tool often bundled with the services provided by credit card processors is real-time credit card payment processing using secure sockets layer (SSL) technology, which encrypts all customer information during the transmission and authorization of online transactions. Another example is an address verification service, which compares the numerical information in customer addresses with records stored by card-issuing banks. Major credit card companies are also adding three-digit codes, called "card verification value systems," to the back of credit cards to assist merchants accepting online and telephone orders determine if a user's card is valid.

© The Regents of the University of California

§10.10 3. Phone and Fax Orders

Companies doing business online often provide customers with multiple ordering options. In addition to online order placement, merchants often establish toll-free telephone and fax numbers to receive orders, which may be linked to a call center open 24 hours a day, seven days a week.

© The Regents of the University of California

§10.11 4. Security Certificates

Security certificates are issued by third party security services to confirm a website's compliance with basic industry security guidelines. Companies that provide security certificates usually do so by subscription. They monitor a merchant's website on an ongoing basis and issue a certificate or a symbol to post at the website. Security certificates are not required by law in order for a merchant to accept orders over the Internet, but it is a good business practice for merchants to obtain certificates to give customers assurance that the data they provide in an e-commerce transaction will remain secure. Moreover, evidence of a company's continued attention to security issues may be an important element of due diligence in a potential joint venture or business acquisition.

© The Regents of the University of California

E. Shopping Cart Services

§10.12 1. Overview

Online shopping carts are electronic order forms. Customers access the form through a hyperlink on a merchant's website. Like physical shopping carts, online carts usually can hold multiple items to be purchased. Shopping cart software automatically calculates and totals a customer's order, including applicable tax and shipping charges; it must be installed on the server that hosts the website or the secure server that accepts ordering information. Online merchants can license shopping cart software directly from the software vendor and host the software on their own. Alternatively, the merchant's website hosting service or credit card processor can provide the shopping cart service. In any event, it is important to ensure that the shopping cart service selected will function properly and can be supported by the merchant's credit card processor.

© The Regents of the University of California

§10.13 2. Evaluating Shopping Cart Services

In evaluating shopping cart services, companies should consider these issues:

- **Security**. Does the shopping cart offer state-of-the-art security and encryption capabilities such as 1024-bit encryption or secure sockets layer (SSL) software?
- **Customizing**. Can the shopping cart be scaled to manage not only the current volume of business but also additional volume as the business expands?
- **Real-time shopping and reporting**. Can customers place orders on a "real time" basis and receive credit card authorization at check out? Can customers check on the status of orders online after the order is placed? There may be additional charges for this option.
- **Multiple-store management**. Does the software permit managing order input for more than one online store? Some programs do not have this capability.
- **Appearance**. Does the software allow the merchant to create a customized user interface with the merchant's logo and special information regarding product categories and shipping methods?
- **Administration**. Can the service handle automatic tax and shipping calculations, customer inquiries and customer service by e-mail, and immediate order confirmation to customers by e-mail?
- **Data management**. How is data stored and backed up? Who is responsible for backup?
- **International capabilities**. Does the shopping cart service accommodate other languages or currencies?

© The Regents of the University of California

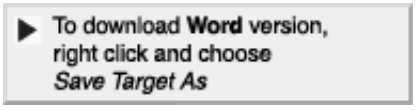
F. Sample Website End User Payment Terms

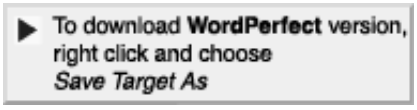
§10.14 1. Introduction

If an Internet website takes orders from customers and processes payments for goods or services online, its terms of use (see §§8.2-8.3) and privacy policy (see §§9.39-9.46) should address issues related to those operations and be tailored to the type of business conducted on the site. The following sample language is intended for use in connection with a subscription-based service, and should be inserted in the website's terms of use.

© The Regents of the University of California

§10.15 2. Form: Sample Clauses re Payment of Subscription Fees





FEES

Some products and services available through or in connection with this Site require that you purchase a subscription or otherwise pay a fee. You hereby authorize the Company and its merchant provider to charge your credit card in advance for all applicable fees incurred by you or on your behalf in connection with the product or service you have chosen to use. You are solely responsible for all charges, fees, duties, taxes, and assessments arising out of any use of your account by you or anyone else using your account. The Company reserves the right to change the amount of, or basis for determining, any fees or charges for services it provides, and to institute new fees, charges, or terms effective upon prior notice to customers. Such new fees, charges, or terms shall not take effect earlier than 30 days after the Company posts such modified fees on the Web site or communicates them to you by e-mail. The Company reserves the right to terminate any account at any time for any reason.

The Company agrees that it will terminate Customer's account upon notice from Customer. If cancellation is received within the first 30 days of Customer signing up for a service, Customer will be refunded all subscription fees for that service, but Customer will still be obligated to pay any other charges incurred. If Customer cancels a service after 30 days of signing up for a service, no refund for unused time on such service will be made. If Customer has a balance due on any account, Customer agrees that the Company can charge these unpaid fees to Customer's credit card.

Your subscription will be automatically renewed. The renewal charge shall be equal to the original signup price, unless otherwise notified in advance by the Company by e-mail to you or as posted on the Company site. Customer will have 30 days after the date that any renewal fee is posted to Customer's charge account to give notice that he or she wishes to cancel his or her subscription. The subscription will be cancelled on receipt of such notification and a credit will be posted to Customer's charge account equal to the latest renewal fee charged.

Customer's right to use the Service is subject to any expenditure limits established by the Company or by Customer's credit card issuer. If payment cannot be charged to Customer's credit card or Customer's charge is returned for any reason, including chargeback, Company reserves the right to either suspend or terminate Customer's access and account, thereby terminating this Agreement and all obligations of Company hereunder.

If Customer has reason to believe that Customer's account is no longer secure (for example, in the event of a loss, theft or unauthorized disclosure or use of Customer's ID, password, or any credit, debit, or charge card number stored), notify the Company of the problem to avoid possible liability for any unauthorized charges to Customer's account.

It is your responsibility to notify the Company if your credit card has changed or has expired and to make appropriate changes or your service may be disconnected or interrupted.

© The Regents of the University of California

§10.16 G. FTC's Mail or Telephone Order Merchandise Rule

When receiving orders over the Internet, by telephone, or by mail order, businesses are required to comply with the FTC's Mail or Telephone Order Merchandise Rule, found at 16 CFR §435.1 and online at http://www.ftc.gov/bcp/edu/pubs/business/adv/bus02.shtm. Under the Rule, a merchant must have a reasonable basis for stating or implying that a product can be shipped within a certain time. If an advertisement, catalog, or web page does not state how many days it will take for the product to ship, the merchant must reasonably believe it can ship the product within 30 days. 16 CFR §435.1(a)(1).

If the merchant cannot ship the product when promised, it must notify the customer and give the customer a right to cancel. For delays of up to 30 days, the merchant may treat the customer's silence as agreement to the delay. For longer or indefinite delays, and second and subsequent delays, the merchant must obtain the customer's consent to the delay. If consent is not obtained, the merchant must promptly refund all the money paid by the customer, without requiring that the customer make a demand for such refund. 16 CFR §435.1(b). The FTC has applied the Rule both to purchased goods and to related rebates or merchandise premiums (free gifts). In its interpretation of the Rule, the FTC states (http://www.ftc.gov/bcp/edu/pubs/business/adv/bus02.shtm):

> When the order is paid for in whole or in part by proofs of purchase, coupons, or other promotional devices, you must provide "reasonable compensation" to the customer for the proofs of purchase plus any shipping, handling, or other charges the customer paid. (The circumstances of each promotion may affect what is deemed to be reasonable.)

For further information, see "Selling on the Internet: Prompt Delivery Rules" at http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt051.shtm and "A Business Guide to the Federal Trade Commission's Mail or Telephone Order Merchandise Rule," located at http://www.ftc.gov/bcp/edu/pubs/business/adv/bus02.shtm.

In *U.S. v Iomega Corp.* (Dec. 9, 1998) Civ Act No. 1:98CV00141C, FTC File No. 972 3023 (reported at http://www.ftc.gov/os/1998/12), the FTC brought an action against a leading manufacturer of portable data storage devices for failing to offer consumers any options regarding delayed delivery, failing to provide prompt refunds when orders were not timely filled, and failing to promptly deliver cash rebates and other premiums to customers. The manufacturer settled and paid a civil penalty of $900,000. Even some of the country's large online retailers have been fined for violations of the Rule. As a result of an FTC investigation titled Project Toolate.com, the agency in July 2000 levied penalties totaling $1.5 million on major retailers for violating the Rule during the previous December holiday season. Macys.com, Inc. was fined $350,000 and required to promote consumer awareness of the Rule by posting banner ads on its site to alert consumers to their rights when shopping online. See *U.S. v Macys.com, Inc.* (July 26, 2000) FTC File No. 0023114 (reported at http://www.ftc.gov/os/2000/07). The FTC also obtained injunctions against Macys.com and other Internet retailers prohibiting future violations and requiring the retailers to file reports demonstrating that they adopted procedures to comply with the Rule. See, *e.g., U.S. v CDnow, Inc.* (July 26, 2000) FTC File No. 0023116; *U.S. v Southdale Kay-Bee Toy, Inc. & KBkids.com LLC* (July 26, 2000) FTC File No. 0023115; *U.S. v Toysrus.com, LLC & Toysrus.com, Inc.* (July 26, 2000) FTC File No. 0023008 (cases reported at http://www.ftc.gov/os/2000/07).

© The Regents of the University of California

II. TAX ISSUES

§10.17 A. Formulation of E-Commerce Tax Policy

Wide-ranging efforts are underway to adapt federal, state, and local tax structures to e-commerce. Governments are concerned that migration of business activities to the Internet may significantly reduce traditional tax revenue streams. At the same time, many are reluctant to hinder the developing online economy with a disproportionate tax burden. To keep the playing field level for competing non-electronic businesses, many jurisdictions try to apply traditional tax structures to online transactions. Conventional tax mechanisms, however, do not easily carry across to e-business transactions, and may add compliance costs that impede the growth of e-commerce.

The most important national efforts concerning taxation of Internet transactions are (1) the Internet Tax Freedom Act (ITFA) (Title XI of Pub L 105-277, 112 Stat 2681, Omnibus Appropriations Act of 1998) (see §10.20), designed to prevent creation of new taxes on Internet transactions, and (2) the Streamlined Sales Tax Project, an interstate effort to simplify sales and use taxes and mitigate the compliance burden and revenue losses caused by out-of-state sales transactions.

© The Regents of the University of California

§10.18 1. International Tax Policy

Traditional tax structures can readily be applied to tangible property, such as manufactured products, bought and sold in international e-commerce transactions. Digital products purchased and shipped over the Internet, such as e-books and software, however, raise novel tax policy questions concerning where the product is purchased and where income is earned.

The World Trade Organization (WTO) and the Organization for Economic Cooperation and Development (OECD) are addressing international e-commerce tax policy. The WTO, established in 1995 as a successor to the General Agreement on Tariffs and Trade, comprises approximately 144 member countries, including Brazil, Canada, China, France, Germany, Japan, South Africa, the United Kingdom, and the United States. The WTO's mission is to help producers of goods and services, exporters, and importers conduct their businesses by ensuring that trade flows freely, smoothly, and predictably. In May 1998, the WTO issued a declaration on e-commerce encouraging the adoption of a program to examine all trade-related issues arising from global e-commerce. As part of that and subsequent declarations, the WTO pledged that its members for the time being would continue to refrain from imposing customs duties on electronic transactions. See WTO Doc. No. 1-5859, Ministerial Declaration, Ministerial Conf.—Fourth Sess., Doha (Nov. 14, 2001), available at http://www.wto.org/english/thewto_e/minist_e/min01_e/mindecl_e.doc.

The OECD provides another international forum at which governments can meet to discuss and develop tax policy. At its Ottawa conference in October 1998, the OECD issued a policy statement entitled "Electronic Commerce: Taxation Framework Conditions," recommending that generally accepted tax policies such as neutrality be followed in formulating tax law for e-commerce. Since then, the OECD has organized and sponsored conferences and international efforts to achieve consensus on e-business taxation. In addition, the organization has created a model tax treaty, which serves as the basis for many tax treaties between nations and provides guidance on how its provisions should be interpreted. See generally http://www.oecd.org.

As part of the Internet Tax Freedom Act (see §10.20), Congress encouraged the president to work through organizations like the WTO and the OECD to keep e-commerce free of burdensome and discriminatory taxes. See Pub L 105-277, §1203, 112 Stat 2681.

© The Regents of the University of California

2. United States Federal Tax Policy

§10.19 a. Role of Treasury Department

In November 1996, the United States Department of the Treasury, Office of Tax Policy, released a paper entitled, "Select Tax Policy Implications of Global Electronic Commerce," available at http://www.ustreas.gov, in which it advocated (1) a neutral policy on e-commerce transactions, treating similar income similarly, and (2) no new or additional taxes on online transactions. The Treasury Department identified the following areas of concern with respect to Internet transactions: jurisdiction for tax purposes, classification of income from digitalized transactions, and administrative and compliance issues arising from the potential for anonymous and untraceable transactions. The subject of jurisdiction for e-commerce transactions is discussed in §§10.22-10.23.

© The Regents of the University of California

§10.20 b. The Internet Tax Freedom Act and Recent Developments

In an attempt to forestall the imposition on e-commerce of a multitude of uncoordinated state and local tax regulations, Congress in 1998 passed the Internet Tax Freedom Act (ITFA) (Title XI of Pub L 105-277, 112 Stat 2681, the Omnibus Appropriations Act of 1998; 47 USC §151, Note). The ITFA placed a 3-year moratorium on the imposition by state and local governments of new taxes on Internet access. Excepted were taxes generally imposed and actually enforced prior to October 1, 1998. The ITFA has been amended several times to extend its term, most recently by the Internet Tax Freedom Act Amendments Act of 2007 (Pub L 110-108, 121 Stat 1024), which extends the term of the tax moratorium until November 1, 2014.

The ITFA established the 19-member Advisory Commission on Electronic Commerce, a group charged with evaluating Internet-related taxation issues. During its 18-month tenure, the commission considered model state legislation providing for uniform application of and exemption from sales and use taxes and ways to simplify federal, state, and local taxes on telecommunication services. Unfortunately, the commission did not reach a consensus on what action the government should take. As of this writing, the appropriate policy on taxation of Internet transactions is still subject to debate. The commission's report to Congress can be found at http://govinfo.library.unt.edu/ecommerce/acec_report.pdf.

It is important to note that (1) the ITFA has no effect on taxes that were imposed before its enactment, (2) preexisting liabilities for existing taxes remain, and (3) the ITFA does not ban taxes on Internet transactions that would otherwise be taxable if they were transacted in a more traditional manner, such as intrastate sales at a retail store or over the telephone. Thus, the effect of the law was to impose a "status quo" on taxes on the Internet as opposed to true "freedom" from taxation.

The congressional Joint Committee on Taxation issued a report titled "Options to Improve Tax Compliance and Reform Tax Expenditures," dated January 27, 2005 (see http://www.jct.gov/s-2-05.pdf), which suggests that the federal government might tax "all data communications services to end users," including broadband, dial-up, fiber, cable modems, cellular, and DSL (digital subscriber line) links. Currently, a 3-percent excise tax is in effect that applies only to traditional telephone service. See IRC §4251. Because of the decreasing popularity of landlines, the Joint Committee on Taxation concluded that it might make sense to expand this tax to new technologies. This report comes soon after the Internal Revenue Service and Treasury Department indicated that they were considering how this same telecommunications tax should be reinterpreted "to reflect changes in technology" used in "telephonic or telephonic quality communications." 69 Fed Reg 40345 (2004).

© The Regents of the University of California

§10.20A c. The Streamlined Sales Tax Agreement

The Streamlined Sales Tax Agreement was developed in 2002 by a committee of tax officials from various states for the purpose of simplifying the administration of state sales taxes by creating uniformity in taxing regimes. For more information, see generally http://www.streamlinedsalestax.org. On October 3, 2005, the Agreement became effective, with 13 states initially complying with its terms (Indiana, Iowa, Kansas, Kentucky, Michigan, Minnesota, Nebraska, New Jersey, North Carolina, North Dakota, Oklahoma, South Dakota, and West Virginia) and 5 more committed to do so in 2007 (Arkansas, Ohio, Tennessee, Utah, and Wyoming).

Although the Streamlined Sales Tax Agreement is not specifically targeted at online businesses, and vendor compliance is voluntary, it reflects increasing concern at the state level for revenues lost on out-of-state purchases, which are increasingly facilitated by the Internet.

© The Regents of the University of California

§10.21 3. California Tax Policy

Currently, state tax policies regarding Internet transactions and access are not uniform. As stated in the report of the House Committee on the Judiciary in the Internet Tax Nondiscrimination Act (H Rep No. 107-240, 107th Cong, 1st Sess (2001)):

> Contrary to the widespread impression that the Internet is a tax-free haven, e-commerce transactions are subject to various state and local taxes. Telecommunications channels such as telephone lines, wireless transmissions, cable, and satellites are subject to taxation. Electronic merchants are required to pay state and local income, licensing, franchise, business activity, and other direct taxes. In addition, physically-present electronic merchants are required to collect and remit applicable sales and use taxes for all intrastate transactions. In short, online transactions are subject to nearly all taxes imposed on traditional brick and mortar enterprises. The only substantive difference between the tax treatment of online and traditional retailers is a state's authority to require nonresident electronic merchants to collect and remit sales and use taxes.

In 1998, the California Legislature, leaning towards tax-neutral policies and protection of the Internet, passed a temporary tax moratorium similar to the ITFA entitled the California Internet Tax Freedom Act (California ITFA) (Rev & T C §§65001-65004). Like the federal ITFA, the California ITFA was not intended to prohibit all taxes on Internet-related transactions. Thus, under the California ITFA, Internet transactions that would be taxed if they occurred at brick-and-mortar retail stores or over the telephone were generally subject to California state and local taxes. Initially set to expire January 1, 2002, the California ITFA was extended until January 1, 2004 by the California Legislature. Stats 2001, ch 343 (SB 394). The California ITFA has now expired. A bill to extend the term of this law until 2010, AB 1791 (2004), did not pass the state legislature.

© The Regents of the University of California

B. Sales and Use Taxes

§10.22 1. General Principles

Sales and use taxes are imposed on retail vendors at the state and local level on transactions involving tangible personal property and certain taxable services. Sales and use taxes typically do not apply to nonretail sales, where the purchaser intends to resell rather than use the property. See Rev & T C §§6001-7226. Forty-five states and the District of Columbia impose sales and use taxes. Counting local governmental authorities, approximately 7500 U.S. taxing jurisdictions collect sales taxes.

If the seller has a nexus with the taxing jurisdiction, the seller is usually required to collect the tax (as a sales tax) and remit it to the relevant state taxing authority. However, in many transactions, particularly mail order and more recently e-business transactions, the vendor may not have physical presence in the jurisdiction in which the tax is imposed. If there is no nexus between the vendor and the taxing jurisdiction and a sales tax is not collected, the purchaser is typically obligated to pay a use tax of an equivalent amount on property or taxable services purchased for use, storage, or consumption within the jurisdiction.

Although the fundamental structure of sales and use taxes in California is similar to that of other states, the rules of each state vary in particular respects. As a result, for interstate e-commerce transactions, rules of other jurisdictions must be examined in order to ensure tax compliance and to enable a business to adopt transactional structures that will minimize tax obligations. For a multi-state business, variations in state and local laws can impose a significant compliance burden. See Sales and Use Taxation of E-Commerce: *State Tax Administrator's Current Thinking with CCH Commentary* (CCH, Chicago, 2000). See also Fields, Understanding and Managing Sales and Use Tax (5th ed CCH, Chicago, 2001).

© The Regents of the University of California

§10.23 2. Constitutional Restrictions on Use Tax Collection Obligations

Questions regarding the constitutionality of state-imposed use taxes arose in *National Bellas Hess, Inc. v Department of Revenue* (1967) 386 US 753, 18 L Ed 2d 505, 87 S Ct 1389, overruled in part by *Quill Corp. v North Dakota* (1992) 504 US 298, 119 L Ed 2d 91, 112 S Ct 1904 (collecting tax from mail order vendor with no physical presence in state violated Due Process and Commerce Clauses). The *Bellas Hess* court set forth a bright-line test requiring that the vendor have a physical presence in the state in order to demonstrate the minimum contacts that due process requires. With regard to the Commerce Clause, the Court held that a vendor whose only contacts with the taxing state are by mail or common carrier could not be required to collect use taxes for the state.

Nearly three decades later, the Court revisited *Bellas Hess* with another out-of-state mail order vendor, Quill Corporation, which faced a use tax imposed by the state of North Dakota. *Quill Corp. v North Dakota* (1992) 504 US 298, 119 L Ed 2d 91, 112 S Ct 1904. Quill had no physical presence in the state (*e.g.,* no outlets or sales representatives), but had sales revenues of nearly $1 million from approximately 3000 customers in North Dakota; it was the sixth largest vendor of office supplies to state residents. The *Quill* Court distinguished the purpose of the due process nexus requirement, intended to require notice or fair warning of government activity, and the Commerce Clause nexus requirement, which was concerned with the burden of state regulations on interstate commerce and the national economy. For the former, the Court abandoned its bright-line physical presence test and adopted a more flexible analysis concerning whether a vendor's contacts with the taxing state made it reasonable to require it to defend a suit in that state. Quill was found to have sufficient minimum contacts to satisfy due process because it purposefully directed its activities to the state residents and its contacts were extensive. With regard to the Commerce Clause, however, the Court reaffirmed its holding in *Bellas Hess* that a state may not burden interstate commerce by requiring that a vendor whose only contacts with the taxing state are by mail or common carrier collect a state use tax.

The conditions in *Quill* are similar to those faced by e-businesses in interstate sales, where the vendor's contacts with a taxing state may be limited to phone lines and Internet links and subsequent delivery of property by mail or common carrier. With its prior position in *Bellas Hess*, however, the Supreme Court in *Quill* left it to Congress to establish legislatively the conditions under which tax obligations can be imposed on remote vendors that deliver taxable goods and services via instrumentalities of interstate commerce.

California e-businesses selling products to residents of other states may be subject to mandatory collection and reporting of such states' sales and use taxes. Local tax resources and authorities should be consulted before engaging in interstate transactions.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/10 E-Commerce Transactions and Tax Issues/§10.24 3. California Sales and Use Taxes

§10.24 3. California Sales and Use Taxes

As a general rule, e-business retail vendors based in California and selling products in California or to Californians are required to collect California sales and use taxes from their customers. See generally Rev & T C §§6001-7176. To facilitate the collection and remittance of state taxes, the California State Board of Equalization (BOE) provides online updates and general information on taxable transactions at its website at http://www.boe.ca.gov. The statewide sales and use tax rate (currently 7.25 percent) is subject to add-on by local taxing districts. Current total sales and use tax rates are listed by California city and county in Publication 71, available at http://www.boe.ca.gov/pdf/pub71.pdf. The BOE also provides online guidance regarding the state's taxation of Internet sales in its Publication 109 entitled "Are Your Internet Sales Taxable?" available at http://www.boe.ca.gov/pdf/pub109.pdf.

The California Internet Tax Freedom Act (California ITFA) (see §10.21) bans discriminatory taxes on Internet access and online computer services and their use. Consistent with the principle of tax neutrality for equivalent transactions, however, California has no general exemption from sales and use taxes for sales made over the Internet. California law imposes a sales tax on all tangible personal property sold at retail in California as a percentage of the purchase price of the property. Rev & T C §6051. Thus, for a vendor located in California, Internet sales of tangible personal property for delivery or use in California are taxed to the same extent as sales of equivalent property made at "brick and mortar" stores.

In addition to the sales tax, the Revenue and Taxation Code imposes an excise tax (*i.e.,* a use tax) on the storage, use, or other consumption in the state of California of tangible personal property purchased from any retailer for storage, use, or other consumption in the state of California. Rev & T C §6201. The use tax rate is the same as the sales tax rate. California's tax code imposes the tax liability on the purchaser, but requires that all retailers "engaged in business" in the state of California and making sales of tangible personal property for storage, use, or other consumption in California collect the tax at the time of the sale and remit the tax to the state, unless the purchaser elects to remit the tax himself. Rev & T C §§6202-6203. Some exceptions apply. See Rev & T C §§6292-6293. A retailer is considered to be engaged in business in the State of California if, among other things (Rev & T C §6203(c)):

- The retailer maintains a business location in California (including temporary locations and locations indirectly maintained through third parties); or
- The retailer has an agent, representative or sales person, independent contractor, or solicitor in California making sales, taking orders, or delivering or installing merchandise.

A vendor is not considered to be "engaged in business" in California solely by reason of "taking of orders from customers in this state through a computer telecommunications network" if the network is not directly or indirectly owned by the retailer and the orders result from the electronic display of products on that network. Rev & T C §6203(d)(1).

Like the statute at issue in *Quill,* California's tax code includes a provision that would require an out-of-state vendor "soliciting orders for tangible personal property by mail if the solicitations are substantial and recurring" in California to collect and remit use taxes on sales made into California. Rev & T C §6203(c)(4). Based on the holding in *Quill,* this section is probably inoperative, but would become operative if federal law is enacted authorizing states to compel out-of-state vendors to collect sales and use taxes even though their only contact with the state is through an instrumentality of interstate commerce such as mail or common carrier.

In *Borders Online, LLC v State Bd. of Equalization* (2005) 129 CA4th 1179, 29 CR3d 176, the court of appeal held that Borders Online was obligated to collect tax on sales of tangible products shipped to California residents, even though it did not have a place of business in California. Its affiliate, Borders, Inc., operated brick-and-mortar stores in California, and the court found that Borders, Inc., acted as Borders Online's representative or agent in the state, bringing Borders Online's sales within the reach of the California taxing authority. 129 CA4th 1199. The following facts supported the finding of an agency relationship: Borders, Inc., was authorized to accept returns for its online affiliate for exchange, store credit, or credit card credit; the two companies engaged in cross-promotional activities, including a link

on the online storefront to borderstores.com, which listed store locations; Borders store employees were encouraged to refer brick-and-mortar customers to Borders Online; and the receipts of Borders, Inc., were printed with the phrase "Visit us online at http://www.borders.com." 129 CA4th at 1195.

© The Regents of the University of California

§10.25 4. California Sales and Use Tax Treatment of Software Sales and Related Services

E-businesses should note that California sales and use tax regulations contain special provisions addressing sales of computers, software, and data processing services. The California Code of Regulations provides guidelines for application of sales and use taxes to transactions consisting of manipulation of consumer-provided data, provision of training and service materials, transfer of computer programs, service charges, pick-up and delivery charges, and rental of computers. 18 Cal Code Regs §1502.

Software can be purchased outright or it can be acquired through a software license agreement that, depending on the agreement terms, may be considered to be a purchase or a lease. In general, the same rules apply to software purchases and software license agreements. Custom software and custom software license agreements are subject to sales and use taxes. 18 Cal Code Regs §1502(f)(2)(A). Custom software is a computer program created and tailored specifically for a particular customer application. The definition includes modifications of prewritten or "canned" software at a charge of 50 percent or more than its original purchase price. 18 Cal Code Regs §1502(f)(1)(B). Canned software is defined as a pre-written program developed for general or repeated sale or lease. 18 Cal Code Regs §1502(f)(1). Canned software and canned software license agreements are taxable if delivered via tangible media such as tape, disk, diskette, or CD-ROM. Canned software is not taxable if delivered electronically.

Maintenance agreements for canned software that are not optional but are required by the seller/licensor as a condition of purchase are considered to be part of the selling price of the software itself and are taxed accordingly. 18 Cal Code Regs §1502(f)(1)(C). If the maintenance agreement is not mandatory, and no tangible personal property transfers to the customer as a part of the maintenance contract, sales and use taxes do not apply. 18 Cal Code Regs §1502(f)(1)(C). Maintenance agreements for custom software are not subject to sales and use taxes. 18 Cal Code Regs §1502(f)(2)(A).

© The Regents of the University of California

11

Strategic Alliances

I. INTRODUCTION §11.1

II. TYPES OF ALLIANCES §11.2

III. FORM: SAMPLE LETTER OF INTENT RE: STRATEGIC ALLIANCE §11.3

IV. SAMPLE STRATEGIC ALLIANCE AGREEMENT
- A. Introduction §11.4
- B. Form: Strategic Alliance Agreement §11.5

V. SAMPLE CO-BRANDING AGREEMENT
- A. Introduction §11.6
- B. Form: Co-Branding Agreement §11.7

© The Regents of the University of California

§11.1 I. INTRODUCTION

The term "strategic alliance" does not have a strict definition at law. The term is sometimes used for marketing purposes to make an agreement or relationship sound unique and special when, in fact, the relationship is merely one of vendor and customer. Often, however, the term is used to describe an arrangement that is something more than a routine contractual relationship. Additional contractual benefits may include access to resources that cannot easily be obtained elsewhere, such as technology, capital, expertise, content, or access to customers. Each side may benefit from speed, efficiency, or other value that the alliance creates. The parties may also share risk, cost, and decision-making authority, as well as use of their respective brands.

Alliances between Internet-based businesses are often created to allow the participants to access their combined customer base for an expanded line of products or services. For example, in 2003, SBC, a telephone services provider, joined forces with Yahoo, an Internet portal, to co-brand high-speed and dial-up Internet services for consumers. In 2000, Amazon.com, an online retailer, and Toys-R-Us, a retailer of children's products, launched a strategic alliance to create a co-branded toy and video games store. In these examples, established businesses joined together to take advantage of their combined strengths to further penetrate a target market. Strategic alliances represent an even more important tool for small undercapitalized businesses, as a means to accelerate growth by leveraging on the combined assets of the alliance partners.

Sections 11.2-11.5 provide an overview of various types of alliances used in the Internet and technology markets, and discuss issues in structuring alliances. A sample letter of intent for an alliance is provided in §11.3 and a model strategic alliance agreement is provided in §11.5. In addition, a sample co-branding agreement is included in §11.7 as an illustration of a relatively common form of strategic business relationship.

© The Regents of the University of California

§11.2 II. TYPES OF ALLIANCES

In general, there are two basic types of strategic alliances. In the first type, an equity-based alliance or joint venture, the parties form a separate business entity and share equity ownership. This form of transaction is best used when new ideas or technology will be contributed to a separate business that will have a life of its own and when the new venture is not directly competitive with the parent entities. This type of alliance is complex and costly to form because it involves the establishment of a new business entity with a new operational, governance, equity, and liability structure, and possibly adverse tax and accounting consequences. If the alliance constitutes a general partnership or joint venture under state law, each party assumes general liability for the debts and liabilities of the entity. Equity-based alliances or joint ventures are often established for offshore distribution of products or content, offshore manufacturing, exploration of new technologies in which the parties benefit from cost sharing, or other collaborative activities involving capital expenditures that warrant establishing a new entity.

A more common type of strategic alliance is a contractual alliance, in which the parties' relationship is based entirely on contract. This result is more flexible for the parties, because they can amend the specifics of their relationship as it matures and potentially exit more easily because an exit does not involve unwinding and dissolving a separate entity. Contractual alliances can be formed for a wide variety of purposes ranging from co-marketing and co-branding of products and services to joint research and development agreements.

An alliance agreement articulates common goals and allocates each party's responsibility, risk, and return. How is this different from any other agreement? Sometimes it isn't. As noted above, the term "alliance" sounds appealing for marketing and is often used to characterize routine business relationships to give them an air of importance. Used properly, this term implies that both sides are joining forces with a common goal that neither is pursuing separately and that each will benefit from the expertise or other advantages that the other brings to the relationship.

Key issues involved in exploring and structuring an alliance include:

- The purpose and anticipated term of the venture;
- Respective roles and allocation of responsibility of the parties;
- Governance, decision-making, and resolution of deadlock;
- The parties' initial and ongoing contributions to the venture (in cash, tangible property, staffing, management, advertising credits, intellectual property, or other forms)
- Allocation of revenue from the venture between the parties;
- Antitrust issues, particularly when the prospective alliance partners are major existing or potential competitors;
- Bankruptcy—addressing what happens if an alliance partner files bankruptcy;
- A software or other technology escrow to protect one party against the failure of the other to perform or to continue to maintain key items of software owned by the first party and licensed to the joint venture;
- Allocation of ownership of intellectual property created in the alliance;
- Exit strategy, ideally tied to a clear definition of success and failure of the venture based on milestones and measurable metrics;
- Tax considerations, especially if the transaction is cross-border or if a new entity is being formed; and
- Export restrictions on any applicable software, encryption, or other technology.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/11 Strategic Alliances/§11.3 III. FORM: SAMPLE LETTER OF INTENT RE STRATEGIC ALLIANCE

§11.3 III. FORM: SAMPLE LETTER OF INTENT RE STRATEGIC ALLIANCE

▶ To download **Word** version, right click and choose *Save Target As*

▶ To download **WordPerfect** version, right click and choose *Save Target As*

_ _[*Date*]_ _
_ _[*Company name*]_ _
_ _[*Address*]_ _
_ _[*City, state, zip*]_ _

Attention:

Re: Letter of Intent re: _ _[*identify relationship*]_ _

Dear _ _[*name*]_ _:

Thank you for taking the time to meet with us and to discuss the possibility of a strategic alliance or other business relationship between _ _[*name of client*]_ _ ("Client") and _ _[*name of other party*]_ _ ("Company"). _ _[*Briefly describe the proposed business relationship.*]_ _ This letter of intent ("Letter of Intent") is intended to set forth the parties' intentions with respect to the proposed relationship, and, if you believe it does so accurately, please countersign where indicated below. The parties' intentions are as follows:

1. TERM. On execution of this Letter of Intent, the parties agree to negotiate in good faith toward the execution of a definitive written agreement (the "Agreement") elaborating the terms of this Letter of Intent. This Letter of Intent will terminate on the earliest to occur of (a) _ _[*number of days, e.g., 180*]_ _ days from the date set forth above, or such longer time as the parties may mutually agree in writing, (b) the execution of the Agreement, or (c) 30 days after one party provides the other party with written notice of its desire to terminate this Letter of Intent.

2. NONEXCLUSIVE AGREEMENT. This Letter of Intent is not exclusive, and either party to this Letter of Intent may enter into negotiations with any third party concerning the subject matter hereof without any accounting or other liability to the other party.

Comment: Consider whether it would be valuable to prohibit the parties from entering into negotiations with third parties for a specified period so that they may explore their possible business transaction without the risk of competing offers. If so, the letter of intent should be exclusive for a stated period of time and the exclusivity clause should be stated to constitute a binding obligation under Paragraph 10 below.

3. OBLIGATIONS OF CLIENT. In connection with the proposed business relationship, Client will _ _[*describe client's obligations*]_ _.

4. OBLIGATIONS OF COMPANY. In connection with the proposed business relationship, Company will _ _[*describe company's obligations*]_ _.

Comment: This form of letter of intent contemplates that the parties' respective obligations will be inserted in numbered subparagraphs of Paragraphs 3 and 4 as applicable. Consider including other important items that have already been agreed on by the parties, such as an allocation of revenue and the geographic territory of the potential alliance.

5. DEFINITIVE AGREEMENT. Client and Company will promptly prepare the Agreement and other basic documents elaborating the terms of this Letter of Intent, including exhibits, schedules, representations and warranties, indemnities, and terms and conditions as are customary in connection with agreements of this type.

6. CONFIDENTIALITY. The parties will promptly execute the Mutual Nondisclosure Agreement attached hereto as Exhibit A, to ensure the confidentiality of all proprietary information exchanged by Client and Company in connection with the proposed business relationship.

Comment: See §§4.20-4.21 for a form of mutual nondisclosure agreement that can be modified for use with this letter of intent.

7. PRESS RELEASES. The parties agree that the signing of this Letter of Intent and the anticipated business relationship is an event that both parties wish to announce by means of a press release or other appropriate public announcement. The parties will issue a mutually satisfactory joint press release (the "Initial Release") on the signing of this Letter of Intent. Except as required by law or applicable listing agreement, neither party will make any public announcement concerning this Letter of Intent or the transaction it contemplates without first obtaining the written consent of the other party. The parties agree to consult one another concerning, and to agree in writing on, the form, content, and timing of any press release or other announcement before the issuance of any such press release or other announcement. Notwithstanding the foregoing, the parties will be permitted to make reference to the matters addressed in this Letter of Intent in other press releases, provided that such references are consistent in substance with the Initial Release.

8. RELATIONSHIP OF THE PARTIES. Nothing contained in this Letter of Intent shall be construed to make one party the partner, joint venturer, principal, agent, or employee of the other party.

9. INTELLECTUAL PROPERTY RIGHTS. Nothing contained in this Letter of Intent shall be construed as granting or conferring any rights by license or otherwise, express or implied, for any patents, copyrights, trademarks, know-how, or other proprietary rights of either party acquired before or after the date of this Letter of Intent.

Comment: Consider the impact of this section on any exploratory work that the parties perform together to investigate the possible alliance. If a new business is being formed in an equity-type joint venture, the parties may be preparing business plans or other strategic documents, the ownership rights to which should be allocated between the parties. In most instances, however, development of intellectual property can be postponed until after the definitive agreements are in place.

10. NONBINDING INTENT. This Letter of Intent sets forth the intent of the parties only, and, except for Paragraphs 6, 7, and 11, which shall be binding on the parties, this letter does not create any binding obligations on or rights in Client or Company. This Letter of Intent shall be superseded by the execution and delivery of the Agreement.

11. EXPENSES. Each party shall be responsible for its own expenses in connection with all matters relating to the proposed transaction. Neither party shall have any liability to the other party based on any failure to consummate the transaction contemplated by this Letter of Intent for any reason.

12. GOVERNING LAW. California law shall govern the interpretation of this Letter of Intent, without reference to conflicts-of-law rules. Any dispute arising out of this Letter of Intent shall be submitted to a state or federal court sitting in _ _[*city or county*]_ _, California, which shall have exclusive jurisdiction over the dispute and to which court's jurisdiction the parties irrevocably submit.

We are excited by the prospect of this transaction and look forward to working with you on the Agreement. If you agree that this Letter of Intent accurately states our intentions, please so indicate by signing and returning the enclosed copy of this Letter of Intent. This Letter of Intent shall expire at 5:00 p.m. California time on _ _[*date*]_ _, unless we have received your signed copy by then.

Very truly yours,

Date: _ _ _ _ _ _

_ _[*NAME OF CLIENT*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

AGREED AND ACCEPTED:

Date: _ _ _ _ _ _

_ _[*NAME OF COMPANY*]_ _,
a _ _[*state of incorporation*]_ _ **corporation**

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

© The Regents of the University of California

IV. SAMPLE STRATEGIC ALLIANCE AGREEMENT

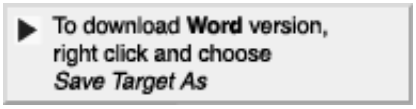
§11.4 A. Introduction

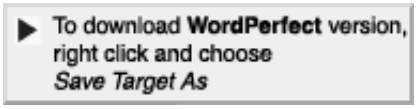
The following sample agreement is a basic alliance agreement for the development and distribution of a software product. In this example, a software developer is working with a website operator to develop products that can be integrated by the website operator into the workings of its site and then distributed to others. The parties share work effort and revenue and allocate intellectual property among themselves.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/11 Strategic Alliances/§11.5 B. Form: Strategic Alliance Agreement

§11.5 B. Form: Strategic Alliance Agreement





STRATEGIC ALLIANCE AGREEMENT

This STRATEGIC ALLIANCE AGREEMENT (the "Agreement") is entered into between _ _[*name of developer*]_ _ ("Developer"), and _ _[*name of website operator*]_ _ ("Website Operator"), as of _ _[*effective date*]_ _ (the "Effective Date"), with reference to the following facts:

A. Developer is a developer and manufacturer of _ _[*describe product*]_ _ (collectively, the "Technology"). Developer has developed the Technology for use in applications that include, without limitation, _ _[*describe applications*]_ _ (the "Field").

B. Website Operator has expertise that includes, without limitation, the integration of third party products into Internet-enabled products for operation on Website Operator's Internet site and for distribution to third parties and has designed and manufactured _ _[*describe products*]_ _ (the "Website Operator Products").

C. Developer from time to time identifies opportunities that require efforts or expertise that are beyond Developer's current expertise or capacity.

D. Website Operator and Developer wish to enter into the strategic alliance relationship contemplated by this Agreement.

NOW, THEREFORE, in consideration of the mutual promises set forth herein, and for good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereby agree as follows:

1. DEFINITIONS. As used in this Agreement, the following terms have the meanings specified below.

1.1. "Bundled Products" means the products that result from the integration and combination of the Technology and the Website Operator Products by the parties under this Agreement.

1.2. "Confidential Information" has the meaning ascribed to it in the Nondisclosure Agreement described in Sections 1.20 and 3.3(c) of this Agreement. Confidential Information also includes the terms and conditions of this Agreement.

1.3. "CPI-U" means the Consumer Price Index for All Urban Consumers for the U.S. City Average for All Items (base index: 1982-84=100). If such index is no longer available, then the parties shall negotiate in good faith regarding a suitable replacement index for use under this Agreement.

1.4. "Customer Referrals" means referrals of prospective Customers, whether by (a) introduction, (b) delivering a name, telephone number, e-mail address, or other contact information, (c) instructing a prospective Customer to contact either Website Operator or Developer, as applicable, or (d) any other means intended to initiate contact between a prospective Customer and either Website Operator or Developer.

1.5. "Customers" means purchasers, licensees, lessees, and end users of the Bundled Products or other products or services provided by a party as contemplated by this Agreement.

1.6. "Developer Intellectual Property" means all worldwide intellectual property rights (including rights under patents, patent applications, trade secret laws, and copyright laws) in the Technology, as well as any Enhancements thereto developed by or on behalf of either party in connection with the parties' performance of this Agreement.

1.7. "Developer Marks" means Developer's trademarks, trade names, and service marks relevant to the Technology and other products and services of Developer to be provided to Website Operator under this Agreement.

1.8. "Developer Pricing Schedule" means Developer's current pricing schedule, attached hereto as Exhibit B, as that pricing schedule may be updated by Developer from time to time in accordance with the terms of this Agreement.

1.9. "Developer Products" means _ _[*define developer's products*]_ _ and any Enhancements to the Developer Products developed and embodied in the Developer Product during the term of this Agreement.

1.10. "Developer Software" means _ _[*define developer's software*]_ _.

Comment: Each party should clearly identify the software and other intellectual property it brings into the alliance to make sure that, if a party later exits the alliance, it is clear which elements belong to which party.

1.11. "Development Copy" has the meaning ascribed to it in Section 3.1(a) below.

1.12. "E-Commerce" means any and all applications in or related to the conduct of business in an online environment, including, without limitation, the buying and selling of products, transactions between two or more businesses, and transactions between businesses and consumers, by any and all digital or electronic means whether now known or hereafter devised, but specifically does not include the Excluded Applications (defined in Section 1.14).

1.13. "Enhancements" means any enhancements, improvements, modifications, or alterations to a party's products or intellectual property conceived or otherwise developed by a party, alone or with others, or by the parties jointly, in connection with the performance of this Agreement.

1.14. "Excluded Applications" means _ _[*define excluded applications*]_ _.

1.15. "Exclusivity Period" means a period of _ _[*number*]_ _ years after the Effective Date of this Agreement, subject to extension as provided for in Section 4 below or by the mutual, written agreement of the parties. The Exclusivity Period as defined herein shall also include any extensions thereto.

1.16. "Implementation Project" means the full scope of work placed under contract to Website Operator or Developer by a Customer with respect to positive identification of individuals using the Technology and/or the Bundled Products. An Implementation Project may include, without limitation, requirements development, system design, customization, deployment, system acceptance, user training, and/or operational system maintenance and support.

1.17. "Implementation Project Revenue" means the total gross revenue collected by a party in connection with an Implementation Project for a Customer. If an Implementation Project is placed under contract in connection with or as part of a larger project with components unrelated to positive identification of individuals, then the contracting party shall separately invoice or itemize those charges that relate to the Implementation Project, and the Implementation Project Revenue shall be that revenue received by the contracting party from such separate invoices or itemized charges.

1.18. "Markets" means _ _[*define markets*]_ _ and such other markets as the parties may mutually agree in writing from time to time during the Term hereof.

Comment: Consider whether there should be geographic or territorial market restrictions on the alliance. Because this agreement contemplates an exclusive arrangement, if one party is unable to execute in a major geographical territory, it may make sense to exclude that territory from coverage under the agreement. Because the Internet is accessible worldwide, however, consider whether the nature of the parties' business would permit compliance (*e.g.,* if the integrated product is being sold and marketed via an Internet website, geographic restrictions may be difficult to enforce).

1.19. "Marks" means the Website Operator Marks (defined in Section 1.24) and the Developer Marks, as applicable.

1.20. "Nondisclosure Agreement" means the mutual nondisclosure agreement attached hereto as Exhibit _ _ and described in greater detail in Section 3.3(c) below.

Comment: See §§4.20-4.21 for a form of mutual nondisclosure agreement that can be modified for use with this alliance agreement.

1.21. "Newly Created Intellectual Property" means all worldwide intellectual property rights (including rights under patents, patent applications, trade secret laws, and copyright laws) in items created by or on behalf of a party, or by the parties jointly, directly in connection with the performance of this Agreement, which items constitute neither Website Operator Intellectual Property (see Section 1.23) nor Developer Intellectual Property (see Section 1.6).

1.22. "Prior Customers" means those persons or entities identified on Exhibit A, attached hereto, who are existing customers of Developer that have purchased and may continue to purchase the Technology within the Territory.

1.23. "Website Operator Intellectual Property" means all worldwide intellectual property rights (including rights under patents, patent applications, trade secret laws, and copyright laws) in the Website Operator Products, as well as any Enhancements thereto developed by or on behalf of either party in connection with the parties' performance of this Agreement.

1.24. "Website Operator Marks" means the trademarks, trade names, and service marks of Website Operator relevant to the Website Operator Products and services of Website Operator to be provided to Developer under this Agreement.

1.25. "Term" has the meaning ascribed to it in Section 5 below.

1.26. "Territory" means the United States and Canada, as well as such other geographic regions as the parties may mutually agree in writing from time to time during the Term hereof.

1.27. "Vertical Market Application" means products or systems relating to the Technology, the Website Operator Products, or the Bundled Products that are developed specifically for use in a single market, and do not have general use or application across a range of markets.

2. PURPOSE AND INTENT. Developer and Website Operator are entering into this Agreement so that they may pursue mutually beneficial business opportunities to sell and implement the Bundled Products in Markets within the Territory. Subject to the terms and conditions set forth in this Agreement, Developer shall supply the Technology to Website Operator, and Website Operator shall integrate the Technology with the Website Operator Products. The parties shall cooperate with respect to integration and subsequent exploitation of the Bundled Products as further described in this Agreement.

3. RESPONSIBILITIES OF THE PARTIES

3.1. RESPONSIBILITIES OF DEVELOPER

(a) TECHNOLOGY AVAILABILITY. Developer shall provide to Website Operator, at no charge to Website Operator, a single copy of the Technology (the "Development Copy"), which Development Copy shall include, at a minimum _ _[*describe included technology*]_ _, as well as such other information or materials as may be necessary for Website Operator to make use of the Technology as contemplated in this Agreement; provided, however, that such information and materials shall not include either the object code or the source code version of the Developer Software. Website Operator shall be entitled to use this Development Copy for demonstration and development purposes only (and not for commercial sale) for Website Operator to integrate it into _ _[*describe product*]_ _ and/or other such products as may be selected by Website Operator in its sole discretion. To assist Website Operator with its integration efforts, Developer shall promptly provide to Website Operator, at no charge to Website Operator, all significant updates (including any and all updates that relate to or have an impact on Website Operator's integration efforts under this Agreement) to the Technology developed by Developer during the Term of this Agreement. On request, Developer shall provide Website Operator with additional copies of the Technology for purposes of development or demonstration at prices at least as favorable as the lowest prices set forth on the Developer Pricing Schedule.

(b) OTHER PRODUCTS. Developer agrees to sell all additional hardware and peripheral support products, including, without limitation, the Developer Product, to Website Operator at Developer's standard system Website Operator prices; provided, however, that such prices shall at all times during the Term be at least as favorable as the lowest prices set forth on the Developer Pricing Schedule. In addition, Developer shall make the Developer Software available to Website Operator for licensing to Customers. Website Operator shall be entitled to use the Developer Software with the Website Operator Products and to incorporate the Developer Software into the Bundled Products, subject to payment of the Developer Software License Fees set forth on the Developer Pricing Schedule.

(c) EXCLUSIVE ARRANGEMENT. During the Exclusivity Period, as described in greater detail in Section 4 below, and except as set forth in Section 4.2 below, Developer shall supply the Technology to Website Operator on an exclusive basis for the Markets within the Territory. Without limiting the foregoing, and except as set forth in Section 4.2 below, Developer shall not, during the Exclusivity Period, provide or offer the Technology or any Integrated Product to any third party in the Territory, or knowingly permit the Technology or any Integrated Product to become available in the Territory, for use in any one or more of the Markets, without the prior written consent of Website Operator.

Comment: Counsel should review any exclusive arrangement, especially between competitors, for compliance with federal and state antitrust law.

(d) INTEGRATION ASSISTANCE. Developer shall use reasonable efforts to assist and advise Website Operator regarding the proper system architecture as it pertains to the Bundled Products, and shall use reasonable efforts to implement any suggestions made by Website Operator that Developer, in its sole discretion, deems to be cost-effective improvements to the Technology.

(e) RIGHT OF FIRST NEGOTIATION. Developer hereby grants to Website Operator a right of first negotiation to act as its primary provider of Bundled Products (the "Preferred Provider") in the Markets outside the Territory for those business opportunities in which Developer uses a third party to provide such Bundled Products and related integration and application services and in which Developer is permitted to choose a third party provider. Such right shall be offered to Website Operator as follows: Developer shall (1) give Website Operator written notice of its intent to identify a Preferred Provider in the new geographic region, along with a full description of the applicable Market services that the Preferred Provider will offer, and (2) if Website Operator indicates in writing within 20 days after receipt of such notice that it desires to pursue negotiations regarding becoming a Preferred Provider, enter into good faith negotiations with Website Operator regarding the Preferred Provider opportunity. If, by 60 days after the date of the notice sent by Developer, the parties have not executed definitive agreements regarding Preferred Provider status, Developer shall be permitted to negotiate with third parties; however, any such negotiations shall be limited to Preferred Provider services substantially similar to those described in the written notice given under this paragraph. Developer may not enter into discussions with any third party regarding establishing that third party as a Preferred Provider in any of the Markets outside the Territory without first complying with this Section 3.1(e).

Comment: Under this agreement, the developer is granting to the website operator the right to create an integrated product and the website operator is doing the bulk of the programming to facilitate the integration. Under this subsection, the developer is attempting to retain the right to be involved in customer projects implementing the integrated product by having a right of first negotiation to provide services to customers of the integrated product. In this way, the developer gains a benefit. If the website operator finds customers for the product, the developer may also gain customers for its own services.

(f) SUPPLY PRIORITY. Developer shall give orders for Technology and other Developer products placed by Website Operator first priority for fulfillment by Developer; provided, however, that Developer shall not be required to breach any preexisting obligations to third parties in order to comply with this Section 3.1(f). The parties shall negotiate in good faith regarding ordering procedures, delivery schedules, and payment terms that will apply to Technology and products ordered hereunder.

Comment: This clause is an example of a priority provision that gives preferential treatment between alliance partners, thus creating an incentive for these relationships. However, these clauses warrant antitrust review.

(g) MAINTENANCE AND SUPPORT. Developer shall provide Website Operator and its Customers with maintenance and support (including, without limitation, technical support, bug fixes, and error corrections) for the Developer Software at Developer's standard rates for such services.

3.2. RESPONSIBILITIES OF WEBSITE OPERATOR

(a) WEBSITE OPERATOR PRODUCTS AVAILABILITY. On execution of this Agreement, Website Operator shall provide to Developer, at no charge to Developer, a single copy of the Integrated Product then being developed hereunder, which copy shall be capable of running on a laptop PC, along with any necessary user documentation, for sales demonstration purposes only (the "Demonstration Copy"). On request, Website Operator shall provide Developer with additional copies of the Demonstration Copy for sales demonstration purposes at the prices set forth on the Pricing Schedule attached hereto as Exhibit _ _, as that Pricing Schedule may be amended from time to time by Website Operator on written notice to Developer. In addition, from time to time during the Term of this Agreement and on request by Developer, Website Operator shall confirm for Developer that Website Operator has provided Developer with the most recent version of any Integrated Product developed under this Agreement; provided, however, that if Website Operator has not provided Developer with the most recent version of an Integrated Product, Website Operator shall provide such most recent version to Developer within 10 business days after the date of Developer's request.

(b) INTEGRATION. Website Operator agrees to use reasonable efforts to integrate the Technology into its Database Product. In connection with the foregoing, Website Operator may, from time to time and in its sole discretion, offer suggestions to Developer for improvements to the Technology.

Comment: Note that, in this example, no objective standard is imposed on the website operator other than "reasonable efforts." Consider requiring performance to be completed by a certain date or in accordance with certain milestones. Here, the website operator is funding its own development work; thus, the lack of deadlines or other performance measures may not be entirely unfair if the website operator is incurring substantial development costs.

3.3. MUTUAL RESPONSIBILITIES

(a) SALES AND MARKETING. The parties acknowledge that certain sales opportunities pursued under this Agreement, whether individually or jointly, may occasionally require the support and cooperation of both parties in a variety of capacities. Developer and Website Operator shall negotiate in good faith regarding their respective participation on such projects, as well as the billable rates that each party shall be entitled to charge the other in connection with each such project. In connection with the foregoing, the parties may cooperate to produce brochures, product descriptions, specifications, and other promotional materials relating to the Bundled Products (collectively, the "Promotional Materials"), which the parties shall be entitled to use and distribute in connection with marketing efforts under this Agreement pursuant to the license granted in Section 4.1(c) below. The parties may use the Promotional Materials in connection with the marketing, promotion, and sale of Bundled Products and other products under this Agreement. Each party may also create its own promotional literature in connection with the marketing, promotion, and sale of the Bundled Products, and may use the other party's Marks and other materials provided by such other party in connection therewith specifically for such purposes; provided, however, that each party shall first submit a copy of any literature so created to the other party for written approval before initial use or distribution. Neither party shall remove or otherwise alter the other party's Marks contained in any materials without the prior written consent of the other party.

(b) PRICING. If a party desires to make any changes to its standard pricing or to the pricing of any products provided to the other party under this Agreement, the party desiring to make such changes shall provide the other party with the updated pricing at least 30 days before the effective date of such changes. In addition, in no event shall such changes affect any Technology, Website Operator Products, Bundled Products, or other products of a party that were ordered by the other party before receiving the notice of changes required by this paragraph.

Comment: This pricing section should also be subject to review for antitrust law compliance.

(c) CONFIDENTIALITY. As a condition to this Agreement, each party agrees to execute and deliver the Nondisclosure Agreement and to maintain the confidentiality of the other party's Confidential Information in accordance with the terms of the Nondisclosure Agreement.

4. LICENSE GRANT AND EXCLUSIVITY

4.1. LICENSE GRANTS

(a) DEVELOPER'S GRANT TO WEBSITE OPERATOR. Developer hereby grants to Website Operator the worldwide, nonexclusive right and license during the Term to use and exploit the Developer Software and, subject to the last sentence of this Section 4.1(a), hereby grants to Website Operator the worldwide, nonexclusive right to integrate the Technology into the Bundled Products and the worldwide, nonexclusive right to make (or have made), import, use, offer for sale and sell (or have sold) such Bundled Products. In addition, subject to the last sentence of this Section 4.1(a), Developer hereby grants to Website Operator, during the Term, the worldwide right to use, offer for sale and sell (or have sold) the Developer Product, independent of the Technology. Notwithstanding anything to the contrary in this Section 4.1(a), unless and until a Release Event (as defined in Section 7 below) occurs, Website Operator shall not have any right independently to make or manufacture, or any right to engage any third person to make or manufacture, the Developer Product, and Website Operator agrees that all Developer Products sold by Website Operator independently or as part of an Integrated Product shall be purchased by Website Operator or its Customer from Developer in accordance with the pricing set forth on the Developer Pricing Schedule.

(b) WEBSITE OPERATOR'S GRANT TO DEVELOPER. Website Operator hereby grants to Developer the worldwide, nonexclusive right and license during the Term to use and exploit the Website Operator Products in connection with Developer's performance of this Agreement and hereby grants to Developer the worldwide, nonexclusive right to offer for sale and sell (or have sold) such Website Operator Products solely in connection with the sale or other exploitation of Bundled Products under this Agreement.

(c) LICENSES TO USE MARKS. Subject to the terms of Section 3.3(a) above, Developer hereby grants to Website Operator, for the Term of this Agreement, the worldwide, nonexclusive right and license to use and reproduce the Developer Marks in connection with the marketing and sales of the Technology, the Developer Products, and the Bundled Products hereunder, and in connection with production of the Promotional Materials described in Section 3.3(a) above. Subject to the terms of Section 3.3(a) above, Website Operator hereby grants to Developer, for the Term of this Agreement, the worldwide, nonexclusive right and license to use and reproduce the Website Operator Marks in connection with the marketing and sales of the Technology, the Developer Products, and the Bundled Products hereunder, and in connection with production of the Promotional Materials described in Section 3.3(a) above. Each party retains all proprietary rights and all goodwill in and to its respective Marks.

4.2. RESTRICTIONS. During the Exclusivity Period, Developer shall not sell, license, or otherwise transfer the Technology or any part thereof in the Markets in the Territory to any third party; provided, however, that notwithstanding the exclusive grant of rights contained in this Agreement:

(a) Developer may continue to sell the Technology to the Prior Customers; provided, however, that (1) Developer shall not modify the Developer Pricing Schedule given to Prior Customers without the prior written consent of Website Operator, which may be withheld by Website Operator in its sole discretion, (2) Developer shall take all necessary action to terminate or not renew its current agreements with the Prior Customers as soon as the right to terminate arises with respect to each such agreement, and (3) Developer shall not take any action to modify any current agreement with a Prior Customer or to assist any Prior Customer in meeting any sales quota required for automatic renewal of that Prior Customer's agreement with Developer.

Comment: This provision ensures that if the developer uses the subject products in its regular operations, it may continue to do business with its existing customers.

(b) Developer may sell the Technology to Customers for use in the Markets in the Territory; provided, however, that Developer may not make sales to any Customer in any 12-month period for which the total revenue received with respect to such Customer exceeds or is reasonably anticipated to exceed _ _[*dollar amount*]_ _.

Comment: This clause limits the developer's ability to create new business and new customers in the contributed software, with the goal of preserving the market for the alliance's products.

(c) If Website Operator (1) decides not to pursue a specific business opportunity relating to this Agreement within the Territory and (2) notifies Developer in writing that it has chosen not to pursue such opportunity, then, on receipt of such written notice, Developer shall be entitled to pursue that specific business opportunity, alone or with a third party. In addition, if Developer inquires in writing of Website Operator whether Website Operator intends to pursue a specific business opportunity relating to this Agreement within the Territory, Website Operator shall respond to such request within a reasonable period of time after receipt of the inquiry.

(d) Subject to its obligations under Section 3.1(e) and Section 3.1(f) above, Developer shall be entitled to sell, license, or otherwise transfer the Technology, or any products incorporating the Technology, outside the Territory and/or outside the Markets.

4.3. EXCLUDED APPLICATIONS. The exclusive rights granted to Website Operator under this Agreement shall not restrict Developer's ability to use, sell, market, develop, or otherwise exploit the Technology with or in any Excluded Applications, or Developer's ability to pursue partnerships with third parties for development and exploitation of Excluded Applications.

5. TERM OF THIS AGREEMENT

5.1. TERM AND TERMINATION. The term of this Agreement (the "Term") shall commence on the Effective Date, and this Agreement shall remain in effect after the Effective Date until terminated in one of the following ways:

(a) Either party may terminate this Agreement, effective immediately on written notice to the other party, if the other party should fail to perform any material obligation under this Agreement or to cure any other material breach of this Agreement within 30 days after receiving written notice of such nonperformance or breach from the terminating party.

(b) Each party shall have the right to terminate this Agreement, effective immediately on written notice to the other party, if the other party should make a general assignment for the benefit of its creditors, commence any voluntary proceeding in bankruptcy, insolvency, or reorganization under bankruptcy laws or laws of debtor's moratorium, or have commenced against it any involuntary proceeding under such laws and such involuntary proceeding is not discharged within 90 days.

5.3. EFFECT OF TERMINATION OF THIS AGREEMENT. On the termination of this Agreement, each party shall retain those limited rights in the Technology, the Developer Software, the Website Operator Products, and the Bundled Products granted hereunder as needed to permit the parties to fulfill Customer agreements under then-existing contractual obligations, subject to each party's obligations to make payments to the other party under this Agreement. The expiration or earlier termination of this Agreement or of the Exclusivity Period shall not affect any Customer, whose rights to and use of the Technology, the Developer Software, the Website Operator Products, and/or the Bundled Products, shall continue without interruption.

6. OWNERSHIP OF INTELLECTUAL PROPERTY

6.1. WEBSITE OPERATOR PRODUCTS. The parties hereby agree that Website Operator shall have sole and exclusive ownership of all worldwide rights in the Website Operator Intellectual Property, including, without limitation, all right, title, and interest in and to the Website Operator Products and all Enhancements thereto. To the extent Developer or any of its agents creates, develops, or suggests any Enhancements to the Website Operator Intellectual Property, Developer hereby assigns and agrees to assign such Enhancements to Website Operator; provided, however, that Website Operator hereby grants and agrees to grant to Developer a perpetual, nonexclusive, worldwide license to use such Enhancements on an internal, noncommercial basis. Should Developer desire to make commercial use of any Enhancement to Website Operator Intellectual Property developed by or on behalf of it hereunder when such use is outside the scope of this Agreement, Developer shall negotiate in good faith with Website Operator regarding such use and shall refrain from such use until the parties reach written agreement on applicable terms and conditions.

6.2. TECHNOLOGY. The parties hereby agree that Developer shall have sole and exclusive ownership of all worldwide rights in the Developer Intellectual Property, including, without limitation, all right, title, and interest in and to the Technology and all Enhancements thereto. To the extent Website Operator or any of its agents creates, develops, or suggests any Enhancements to the Developer Intellectual Property, Website Operator hereby assigns and agrees to assign such Enhancements to Developer; provided, however, that Developer hereby grants and agrees to grant to Website Operator a perpetual, nonexclusive, worldwide license to use such Enhancements on an internal, noncommercial basis. Should Website Operator desire to make commercial use of any Enhancement to Developer Intellectual Property developed by or on behalf of it hereunder when such use is outside the scope of this Agreement, Website Operator shall negotiate in good faith with Developer regarding such use and shall refrain from such use until the parties reach written agreement on applicable terms and conditions.

6.3. JOINT OWNERSHIP. The parties hereby agree that Website Operator and Developer shall have equal joint ownership of all Newly Created Intellectual Property. Neither party shall be required to make an accounting or pay any royalties to the other party with regard to the Newly Created Intellectual Property.

6.4. FURTHER ASSURANCES. From time to time, each party hereto shall execute and deliver such instruments as may be reasonably necessary to carry out the purposes and intent of this Agreement. In addition, each party shall promptly disclose all Enhancements to the other party and shall perform all acts necessary or desirable to assist such other party in obtaining and enforcing the full benefits, enjoyment, rights, and title in the Enhancements throughout the world.

7. ESCROW AGREEMENT. The parties agree to enter into a standard escrow agreement for the Developer Technology in the form attached as Exhibit _ _ hereto (the "Escrow Agreement") with a reputable, national escrow agent agreed on in writing by the parties. In connection with the Escrow Agreement, Developer shall deposit with the escrow agent all tangible intellectual property relevant to this Agreement, including, but not limited to, all source code embodied in the Technology and any other information necessary to maintain and update the Technology, and shall promptly update the escrow deposit as the Technology is updated. The intellectual property deposited into escrow shall become available to Website Operator on the occurrence of certain events (the "Release Events") described in greater detail in the Escrow Agreement. In addition, except as expressly provided in the Escrow Agreement, Developer shall be responsible for payment of all fees in connection with the Escrow Agreement, including, without limitation, all fees for establishing and maintaining an escrow account and for depositing materials into such account; provided, however, that Website Operator shall reimburse Developer for 50% of such fees on Developer's presentation to Website Operator of suitable documentation of such fees.

Comment: See chap 15 for a form of source code escrow agreement that can be modified for use in connection with this alliance agreement.

8. LICENSE FEES AND OTHER CONSIDERATION

8.1. LICENSE FEES. The license fees payable by Website Operator to Developer for use of the Developer Software and exploitation of the Bundled Products by Website Operator (or its reseller or other designee) for each Implementation Project conducted by Website Operator shall be based on the total Implementation Project Revenue received by Website Operator from such Implementation Project. Similarly, the license fees payable by Developer to Website Operator for use of the Website Operator Products and exploitation of the Bundled Products by Developer (or its reseller or other designee) for each Implementation Project conducted by Developer shall be based on the total Implementation Project Revenue received by Developer from such Implementation Project. The license fees payable hereunder shall be as set forth in the Schedule of Implementation, Project License Fees, on Exhibit _ _ attached hereto, as that Exhibit may be amended from time to time by mutual written agreement of the parties. For purposes of this Section 8.1, a party "conducts" an Implementation Project by acting as the prime contractor on the Implementation Project, contracting with a Customer for implementation of Bundled Products, or otherwise taking responsibility for collection of revenue from the Customer.

8.2. CROSS-REFERRAL FEES. In addition to the license fees payable in accordance with Section 8.1 above, each party shall compensate the other party for Customer Referrals provided by one party to the other, if such Customer Referrals result in sales or licenses of products (including, without limitation, the Bundled Products, the Technology, the Website Operator Products, and Developer Products sold independently of any sale or license of Bundled Products). Compensation for Customer Referrals under this Section 8.2 shall be calculated as a percentage of the total revenue that the nonreferring party actually collects from the Customer Referral. The relevant percentages and applicable tiers of revenue are set forth in the Schedule of Customer Referral Fees on Exhibit _ _ attached hereto, as that Exhibit may be amended from time to time by mutual written agreement of the parties.

8.3. THIRD PARTY REFERRAL FEES. When a party or both parties receive a Customer Referral from a third party not employed by or otherwise affiliated with either party, Website Operator and Developer shall negotiate in good faith regarding a referral fee, if any, to be paid to the third party and any referral fees that might be due to either Website Operator or Developer in connection with the third party referral.

8.4. DEVELOPER PRODUCT LICENSE FEES. If, following a Release Event, Website Operator (or a subcontractor designated by Website Operator) should commence manufacture and sale of the Developer

Product, then Website Operator shall pay to Developer a license fee for such manufacture and sale equal to 20% of the price for the Developer Product set forth in the most recent Developer Pricing Schedule (the "List Price") (regardless of the price at which Website Operator actually sells any Developer Product), which List Price shall be increased automatically by a percentage equal to the percentage increase, if any, between the CPI-U on the date of the Release Event and the CPI-U on the date that is 12 months after that date. When such adjustment is made, the revised price shall become the List Price. Thereafter, the adjustment provided for in this Section 8.4 shall be made on an annual basis on the yearly anniversary of the Release Event.

8.5. PAYMENT TERMS. All amounts due to a party under this Agreement, whether in connection with license fees, product purchases, referral fees, or other consideration, shall be payable within 30 days after receipt of payment from a Customer or other third party giving rise to a payment obligation under this Agreement, together with a statement explaining the basis for any and all payments being made at such time. For products ordered by a party for its own use under Section 3.1(a), 3.1(b) or 3.2(a) above, payment shall be due within 30 days after receipt of an invoice for the ordered products. For Customer payments to a party (the "receiving party") in an amount less than the total amount due from such Customer, the receiving party's obligation to the other party under this section shall be adjusted on a pro rata basis. Any amounts payable by a receiving party under this section that remain unpaid after the due date for payment shall be subject to a late charge equal to the lesser of (a) 1.5% per month from the due date until the date of payment, or (b) the maximum amount permitted by law.

9. REPRESENTATIONS AND WARRANTIES

9.1. MUTUAL REPRESENTATIONS AND WARRANTIES. Each party represents and warrants that (a) it has the right to enter into this Agreement and to perform fully its obligations hereunder; and (b) the making of this Agreement does not violate any agreement existing between it and any other person or entity.

9.2. PRODUCT WARRANTIES. The parties shall negotiate in good faith regarding the product warranty or warranties that will apply to the Bundled Products. Each party shall provide the other party with any and all standard product warranties, which the parties shall be entitled to pass through to their Customers. Developer agrees to honor such warranties. To the extent that any Customer requests or requires product warranties that are more extensive than the parties' standard warranties, the parties shall exercise reasonable efforts to accommodate such Customer's request, and shall negotiate in good faith regarding the allocation of any additional costs that accommodating such Customer's request might entail.

9.3. OTHER WARRANTIES

(a) BY DEVELOPER. Developer represents, warrants, and covenants that (1) it will comply with all applicable laws, rules, and regulations in its performance of this Agreement, its use and operation of the Website Operator Products and the Bundled Products, and its cooperation in the development of the Bundled Products as set forth in this Agreement; (2) it is the owner of, or otherwise has the right to license and distribute, the Developer Intellectual Property, and such Developer Intellectual Property does not willfully violate or willfully infringe on any intellectual property right of any third party; and (3) it will use the Bundled Products in accordance with any written instructions provided by Website Operator and with any appropriate standards. DEVELOPER MAKES NO OTHER WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

(b) BY WEBSITE OPERATOR. Website Operator represents, warrants, and covenants that (1) it will comply with all applicable laws, rules, and regulations in its performance of this Agreement, its use and operation of the Website Operator Products and the Bundled Products, and its cooperation in the development of the Bundled Products as set forth in this Agreement; (2) it is the owner of, or otherwise has the right to license and distribute, the Website Operator Intellectual Property, and such Website Operator Intellectual Property does not willfully violate or willfully infringe on any intellectual property right of any third party, and (3) it will use the Developer Products in accordance with manufacturer's instructions and appropriate standards. WEBSITE OPERATOR MAKES NO OTHER WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

10. INDEMNIFICATION AND LIMITATION OF LIABILITY

10.1. GENERAL INDEMNIFICATION

(a) BY WEBSITE OPERATOR. Website Operator shall indemnify, defend, and hold harmless Developer, its directors, shareholders, officers, agents, employees, successors, and assigns from and against any and all liabilities, obligations, costs, losses, or expenses of whatever kind or nature (including without limitation reasonable attorney fees and expenses and other litigation expenses), arising from, in connection with, or related in any way, directly or indirectly, to any negligent act or omission by Website Operator, or to any breach by Website Operator of this Agreement or of its representations or warranties under this Agreement.

(b) BY DEVELOPER. Developer shall indemnify, defend, and hold harmless Website Operator, its directors, shareholders, officers, agents, employees, successors, and assigns from and against any and all liabilities, obligations, costs, losses, or expenses of whatever kind or nature (including without limitation reasonable attorney fees and expenses and other litigation expenses), arising from, in connection with, or related in any way, directly or indirectly, to any negligent act or omission by Developer, or to any breach by Developer of this Agreement or of its representations or warranties under this Agreement.

10.2. INTELLECTUAL PROPERTY INDEMNIFICATION

(a) BY DEVELOPER. Developer, at its expense, shall indemnify, defend, and hold harmless Website Operator, its directors, shareholders, officers, agents, employees, successors, and assigns (collectively, "Website Operator Indemnitees") from and against any and all liabilities, obligations, costs, losses, or expenses of whatever kind or nature (including, without limitation, reasonable attorney fees and expenses and other litigation expenses), arising from or related to any claim that the Technology, the Developer Intellectual Property, or any other materials furnished by Developer under this Agreement infringe a copyright, trade secret, trademark, service mark, or other similar proprietary right of any person. The foregoing obligation shall only apply to those Enhancements to the Developer Intellectual Property that Developer provides to Website Operator under Section 3.1(a) above, and shall not otherwise apply to any Enhancements to the Developer Intellectual Property. Developer shall pay any and all costs, damages, and attorney fees awarded against Website Operator Indemnitees, provided Website Operator Indemnitees notify Developer of any such claim, do not agree to any settlement of such claim without Developer's consent, and agree to any such settlement reasonably proposed by Developer. Notice of any claim hereunder shall be given promptly after any Website Operator Indemnitee becomes aware of such claim; provided, however, that the failure of any Website Operator Indemnitee to give notice as provided in this Section 10.2 shall not relieve Developer of its obligations under this Section 10.2, except to the extent that Developer is actually prejudiced by such failure to give notice. Should the Technology or the Developer Intellectual Property become, or in Developer's opinion be likely to become, the subject of a claim of infringement, Developer shall either (1) procure for Website Operator (including its Customers) the right to continue to use the Technology or the Developer Intellectual Property, or (2) replace, or otherwise modify, the Technology or the Developer Intellectual Property to make it noninfringing, or obtain a reasonable substitute product for the Technology or the Developer Intellectual Property, provided that any replacement, modification, or substitution under this paragraph does not effect a material change in the functionality of the Technology or the Developer Intellectual Property.

(b) BY WEBSITE OPERATOR

(1) INDEMNIFICATION. Website Operator, at its expense, shall indemnify, defend, and hold harmless Developer, its directors, shareholders, officers, agents, employees, successors, and assigns (collectively, "Developer Indemnitees") from and against any and all liabilities, obligations, costs, losses, or expenses of whatever kind or nature (including, without limitation, reasonable attorney fees and expenses and other litigation expenses), arising from or related to any claim that the Website Operator Products, the Website Operator Intellectual Property, or any other materials furnished by Website Operator hereunder infringe a copyright, trade secret, trademark, service mark, or other similar proprietary right of any person. The foregoing obligation shall only apply to those Enhancements to the Website Operator Intellectual Property that Website Operator provides to Developer under Section 3.2(a) above, and shall not otherwise apply to any Enhancements to the Website Operator Intellectual Property. Website Operator shall pay any and all costs, damages, and attorney fees awarded against Developer Indemnitees, provided that Developer Indemnitees notify Website Operator of any such claim, do not agree to any settlement of such claim without Website Operator's consent, and agree to any such settlement reasonably proposed by Website Operator. Notice of any claim hereunder shall be given promptly after any Developer Indemnitee becomes aware of such claim; provided, however, that the failure of any Developer Indemnitee to give notice as provided in this Section 10.2 shall not relieve Website Operator of its obligations under this Section 10.2, except to the extent that Website Operator is actually prejudiced by such failure to give notice.

(2) ACTION ON CLAIM OF INFRINGEMENT. Should the Website Operator Products or the Website Operator Intellectual Property become, or in Website Operator's opinion be likely to become, the subject of a claim of infringement, Website Operator shall either (A) procure for Developer (including its Customers) the right to continue to use the Website Operator Products or the Website Operator Intellectual Property, or (B) replace, or otherwise modify, the Website Operator Products or the Website Operator Intellectual Property to make it (or them) noninfringing, or obtain a reasonable substitute product for the Website Operator Products or the Website Operator Intellectual Property, provided that any replacement, modification, or substitution under this paragraph does not effect a material change in the functionality of the Website Operator Products or the Website Operator Intellectual Property.

11. LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT SHALL EITHER PARTY BE RESPONSIBLE FOR ANY INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES OF ANY KIND, INCLUDING DAMAGES FOR LOST GOODWILL, LOST PROFITS, LOST BUSINESS, OR OTHER INDIRECT ECONOMIC DAMAGES, AND FURTHER INCLUDING INJURY TO PROPERTY, WHETHER SUCH CLAIM IS BASED ON CONTRACT, NEGLIGENCE, TORT (INCLUDING STRICT LIABILITY), OR OTHER LEGAL THEORY, AS A RESULT OF A BREACH OF ANY WARRANTY OR ANY OTHER TERM OF THIS AGREEMENT, AND REGARDLESS OF WHETHER A PARTY WAS ADVISED OR HAD REASON TO KNOW OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE. As some jurisdictions do not allow the exclusion or limitation of warranties or incidental or consequential damages, the foregoing limitations or exclusions may not apply.

12. MISCELLANEOUS

12.1. AMENDMENT. This Agreement may not be amended, except by a writing signed by both parties.

12.2. ASSIGNMENT; BINDING AGREEMENT. This Agreement and the rights and obligations herein may not be assigned or otherwise transferred by either party, in whole or in part, whether voluntarily or by operation of law, including by way of sale of assets, merger, or consolidation, without the prior written consent of the other party. Subject to the foregoing, this Agreement shall be binding on and shall inure to the benefit of the parties and their respective successors and assigns.

12.3. ATTORNEY FEES. If either party institutes or participates in a legal or equitable proceeding against the other seeking to enforce or interpret this Agreement, the nonprevailing party in the proceeding shall pay the prevailing party's costs, expert, and professional fees, and attorney fees, including costs and fees on appeal. This payment obligation of the nonprevailing party shall be deemed to accrue beginning on the date of commencement of such proceeding.

12.4. COUNTERPARTS. This Agreement may be executed in counterparts, each of which so executed shall be deemed to be an original and all such counterparts together shall constitute one and the same agreement.

12.5. FORCE MAJEURE.

(a) Neither party shall be liable in damages, nor shall be subject to termination of this Agreement by the other party, for any delay or default in performing any nonmonetary obligation hereunder if that delay or default is due to any cause beyond the reasonable control and without fault or negligence of that party; provided that, in order to excuse its delay or default hereunder, a party shall notify the other of the occurrence or the cause, specifying the nature and particulars thereof and the expected duration thereof; and provided, further, that within 15 calendar days after the termination of such occurrence or cause, such party shall give notice to the other party specifying the date of termination thereof. All obligations of both parties shall return to being in full force and effect on the termination of such occurrence or cause (including without limitation any payments that became due and payable hereunder prior to the termination of such occurrence or cause).

(b) For the purposes of this Section, a "cause beyond the reasonable control" of a party shall include, without limiting the generality of the phrase, any act of God, act of any government or other authority or statutory undertaking, fire, explosion, accident, power failure, flood, earthquake, riot, or war (declared or undeclared).

(c) NOTICE. Any notice required or permitted under the terms of this Agreement or required by law must be in writing and must be (1) delivered in person, (2) sent by first class registered mail, or air mail, as appropriate, or (3) sent by overnight air courier, in each case properly posted and fully prepaid to the appropriate address

set forth below. Either party may change its address for notice by notice to the other party given in accordance with this Section. Notices shall be considered to have been given at the time of actual delivery in person, 3 business days after deposit in the mail as set forth above, or 1 day after delivery to an overnight air courier service.

If to the Developer:
_ _[*Name*]_ _
_ _[*Address*]_ _

If to the Website Operator:
_ _[*Name*]_ _
_ _[*Address*]_ _

12.6. WAIVER. Any waiver of the provisions of this Agreement or of a party's rights or remedies under this Agreement must be in writing to be effective. Failure, neglect, or delay by a party to enforce the provisions of this Agreement or its rights or remedies at any time shall not be construed or deemed to be a waiver of such party's rights under this Agreement and shall not affect the validity of the whole or any part of this Agreement or prejudice such party's right to take subsequent action.

12.7. SEVERABILITY. If any term, condition, or provision in this Agreement is found to be invalid, unlawful or unenforceable to any extent, the parties shall endeavor in good faith to agree to such amendments that will preserve, as far as possible, the intentions expressed in this Agreement. If the parties fail to agree on such an amendment, such invalid term, condition, or provision shall be enforced to the maximum extent permitted by law or, if not enforceable, shall be severed from the remaining terms, conditions, and provisions, which shall remain in full force and effect.

12.8. ENTIRE AGREEMENT. This Agreement supersedes all prior discussions, representations, warranties, and agreements, both written and oral, among the parties with respect to the subject matter hereof, and, together with the Nondisclosure Agreement, contains the sole and entire agreement among the Parties with respect to the subject matter hereof.

12.9. HEADINGS. The headings herein used are for convenience purposes only and shall not be used to construe the meaning of this Agreement in any respect.

12.10. GOVERNING LAW. This Agreement shall be interpreted and construed in accordance with the laws of the State of California and the United States of America, without regard to its conflicts-of-law principles.

12.11. RELATIONSHIP. The relationship of the parties under this Agreement is one of independent contractors, and no agency, partnership, joint venture, or similar relationship is created hereby. Except as specifically authorized, neither party shall have any authority to assume or create obligations on the other party's behalf. Neither party shall take any action that has the effect of creating the appearance of its having such authority.

12.12. PRESS RELEASES. The parties agree that the signing of this Agreement is an event that both parties wish to announce by means of a press release or other appropriate public announcement. The parties shall issue a mutually agreed on joint press release (the "Initial Release") on the signing of this Agreement. Except as required by law or applicable listing agreement, neither party shall make any public announcement concerning this Agreement or the transactions contemplated hereunder without first obtaining the written consent of the other party. The parties agree to consult one another concerning, and to agree in writing on, the form, content, and timing of any press release or other announcement before the issuance of any such press release or other announcement. Notwithstanding the foregoing, the parties shall be permitted to make reference to the matters addressed in this Agreement in other press releases, provided that such references are consistent in substance with the Initial Release.

12.13. ARBITRATION. Any controversy or claim between the parties hereto arising out of or related to this Agreement or the breach thereof shall be settled by arbitration. The arbitration shall be conducted under the then current Commercial Rules of the American Arbitration Association ("AAA Rules"). With respect to any arbitration proceeding held hereunder, either party has the right to opt for expedited arbitration under the AAA Rules. In addition to the powers conferred by the AAA rules, the arbitrator shall have authority to order such other discovery as he or she deems appropriate for a full and fair hearing of the case. Within 10 days after the

demand for arbitration is given, the parties shall select a single neutral arbitrator to preside over the arbitration proceeding. If the parties fail to select an arbitrator within such 10-day period, such arbitrator shall be chosen by a court of competent jurisdiction. The arbitrator's decision shall be final and binding, and the award so rendered may be filed in any court having jurisdiction. The costs of arbitration shall be borne by the losing party. The provisions of this Section shall survive the expiration or earlier termination of this Agreement.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the Effective Date.

Date: _ _ _ _ _ _

_ _[*NAME OF DEVELOPER*]_ _**,**
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

_ _[*Developer's address*]_ _

Date: _ _ _ _ _ _

_ _[*NAME OF WEBSITE OPERATOR*]_ _**,**
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

_ _[*Website Operator's address*]_ _

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/11 Strategic Alliances/ V. SAMPLE CO-BRANDING AGREEMENT/§11.6 A. Introduction

V. SAMPLE CO-BRANDING AGREEMENT

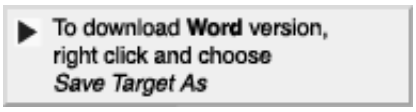
§11.6 A. Introduction

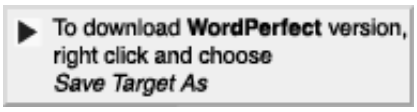
Under a co-branding agreement, a website operator with a developed website typically creates a co-branded page with a major sponsor with a nationally recognized brand name. The co-branded page is accessible through the web page of the sponsor or, if desired, either party. The parties' agreement usually covers the parties' financial relationship concerning revenues from the co-branded page.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/11 Strategic Alliances/§11.7 B. Form: Co-Branding Agreement

§11.7 B. Form: Co-Branding Agreement





CO-BRANDING AGREEMENT

This Co-Branding Agreement (this "Agreement"), dated as of _ _[*date*]_ _, is between _ _[*name of website operator*]_ _, a California corporation having its principal place of business at _ _[*address*]_ _ ("Website Operator"), and, _ _[*name of sponsor*]_ _, a _ _[*state of incorporation*]_ _ corporation having its principal place of business at _ _[*address*]_ _ ("Sponsor").

RECITALS

A. Website Operator provides access to applications and other information and content regarding selecting and applying to and attending colleges and graduate and professional degree programs to end users via the World Wide Web; and

B. Sponsor wishes to obtain sponsorship placement on Website Operator's website and access to certain information pertaining to Website Operator's end users.

NOW, THEREFORE, the parties agree as follows:

1. DEFINITIONS. Wherever used in this Agreement with initial letters capitalized, the following terms shall have the following meanings:

1.1. "Co-Branded Pages" means pages of the Website Operator Website, to be developed under Section 2.2 of this Agreement and hosted on the Website Operator Website, that display both the Website Operator Brand Features and the Sponsor Brand Features, along with such Sponsor Content, Website Operator Content, and other content as the parties may agree upon.

1.2. "Confidential Information" means information of either party (whether of a technical, business, or other nature) that the other party knows or reasonably should know to be confidential or proprietary information of such party.

1.3. "Intellectual Property Rights" means any patent, copyright, rights in Trademarks, trade secret rights, moral rights, and other intellectual property or proprietary rights arising under the laws of any jurisdiction.

1.4. "Exclusive Category" means those product and/or service categories identified on Exhibit A attached to this Agreement.

1.5. "Sponsor Brand Features" means the Sponsor Marks and Sponsor's distinct brand elements that appear from time to time in Sponsor's properties, ventures, and services worldwide and are protected under U.S. copyright law or for which Sponsor has established trademark, service mark, or trade dress rights, and any modifications to the foregoing that may be created during the term of this Agreement.

1.6. "Sponsor Content" means any information, materials, or content supplied by or on behalf of Sponsor, whether directly or indirectly, for use on the Co-Branded Pages.

1.7. "Sponsor Marks" means those Trademarks of Sponsor set forth on Exhibit B attached hereto and such other Trademarks (if any) as Sponsor may from time to time notify Website Operator in writing to be "Sponsor Marks" within the meaning of this Agreement.

1.8. "Sponsor Website" means that Website, the primary home page for which is located at _ _[*URL*]_ _, and any successor or replacement of that Website.

1.9. "Term" means the term of this Agreement as provided in Section 4.1.

1.10. "Trademarks" means any trademarks, service marks, trade dress, trade names, corporate names, proprietary logos or indicia, and other source or business identifiers.

1.11. "Website" means, with respect to any person or entity, all points of presence or services maintained by such person or entity on the Internet (including, without limitation, the World Wide Web) or on any successor public data network. With respect to any Website maintained on the World Wide Web, "Website" includes all HTML pages (or similar unit of information presented in any relevant data protocol) that either (a) are identified by the same second-level domain (such as .com) or by the same equivalent level identifier in any relevant address scheme, or (b) contain branding, graphics, navigation, or other characteristics such that a user reasonably would conclude that the pages are part of an integrated information or service offering.

1.12. "Website Operator Brand Features" means the Website Operator Marks and Website Operator's distinct brand elements that appear from time to time in Website Operator's properties, ventures, and services worldwide and are protected under U.S. copyright law or for which Website Operator has trademark, service mark, or trade dress rights, and any modifications to the foregoing that may be created during the term of this Agreement.

1.13. "Website Operator Content" means any information, materials, or content developed by Website Operator for use on the Sponsor Website.

1.14. "Website Operator Marks" means those Trademarks of Website Operator set forth in Exhibit B attached hereto and such other Trademarks as Website Operator may from time to time notify Sponsor to be "Website Operator Marks" within the meaning of this Agreement.

1.15. "Website Operator Website" means that Website, the primary home page for which is located at _ _[*URL*]_ _, and any successor or replacement of that Website.

2. CONTENT, CO-BRANDING, AND LICENSES

2.1. CREATION OF CONTENT. Following the execution of this Agreement, Website Operator and Sponsor shall work in good faith to develop the content specified in Exhibit C attached to this Agreement. All content to be included on the Co-Branded Pages shall be required to comply with Website Operator's generally applicable content and technical guidelines.

Comment: This provision contemplates that both parties will work together to create content but that all content must comply with the website developer's requirements. Consider attaching those guidelines to the agreement and establishing a mechanism for updating them if needed.

2.2. CO-BRANDED PAGES. Following the execution of this Agreement, Website Operator and Sponsor shall work in good faith to develop the Co-Branded Pages, which may include all or part of the Sponsor Content and/or the Website Operator Content. The Co-Branded Pages shall have the specifications set forth on Exhibit C attached to this Agreement. The Co-Branded Pages shall be required to comply with Website Operator's generally applicable content and technical guidelines. Sponsor shall supply Sponsor Content and Sponsor Brand Features as the parties agree to include in the Co-Branded Pages. Following the development thereof, Website Operator shall use commercially reasonable efforts to post and maintain the Co-Branded Pages on the Website Operator Website. Website Operator may from time to time, in consultation with Sponsor, update and modify the Co-Branded Pages but may not change Sponsor Content or Sponsor Brand Features, or do anything else with them, without Sponsor's prior written consent.

Comment: There are no strict milestones or deadlines in this sample agreement. If applicable, consider placing them in an exhibit to the agreement and tying all development efforts to performance of the milestones. Make sure to specify what, if any, consequences will occur if a milestone is missed.

2.3. SPONSOR'S LICENSE TO WEBSITE OPERATOR. Subject to Section 2.5, Sponsor hereby grants to Website Operator a nonexclusive, revocable, nontransferable, royalty-free, worldwide license to (a) use, reproduce, publish, perform, and display the Sponsor Marks and Sponsor Brand Features on the Co-Branded Pages; (b) link to the Sponsor Website from the Co-Branded Pages and/or the Website Operator Website that

contains the Co-Branded Pages; and (c) use, reproduce, publish, perform, and display the Sponsor Content in and on the Co-Branded Pages. All goodwill arising out of Website Operator's use of any of the Sponsor Marks shall inure solely to the benefit of Sponsor.

2.4. WEBSITE OPERATOR'S LICENSE TO SPONSOR. Subject to Section 2.5, Website Operator hereby grants to Sponsor a nonexclusive, nontransferable, royalty-free, worldwide license to (a) use, reproduce, publish, perform, and display the Website Operator Marks and Website Operator Brand Features on the Sponsor Website in connection with the logo link contemplated by Section 2.1, and, in connection with its promotional and marketing activities contemplated by Section 2.6; and (b) use, reproduce, publish, perform, and display the Website Operator Content on the Sponsor Website or other Sponsor properties as mutually agreed by the parties. All goodwill arising out of Sponsor's use of any of the Website Operator's Marks shall inure solely to the benefit of Website Operator.

2.5. APPROVAL OF TRADEMARK USAGE. Website Operator shall not use or exploit in any manner any of the Sponsor Marks or Sponsor Brand Features, and Sponsor shall not use or exploit in any manner any of the Website Operator Marks or Website Operator Brand Features, except in such manner and media as may be specified in the other party's trademark usage and branding guidelines or as the other party may consent to in writing. Either party may revise such guidelines or revoke or modify any such consent on written notice to the other party.

2.6. PROMOTION OF WEBSITE OPERATOR SERVICES. Commencing on the date of this Agreement and throughout the Term, Sponsor shall use its commercially reasonable efforts (subject to the terms of this Agreement) to promote and market Website Operator and the Website Operator Website generally. In addition, Sponsor shall perform the specific promotional and marketing services specified on Exhibit D attached to this Agreement.

Comment: Co-branding agreements tend to impose vague standards on the parties, because their primary motivation is marketing-related and the juxtaposition of the parties' brands creates substantial value for the parties. Accordingly, marketing sensitivities may make it difficult to reach agreement concerning specific deadlines for performance of marketing services and penalties for nonperformance.

2.7. EXCLUSIVE SPONSORSHIP. During the Term, Website Operator shall not grant any third party any right to sponsor any products or services in the Exclusive Category on or through the Website Operator Website. For the avoidance of doubt, the parties acknowledge that the foregoing restriction applies only to persistent sponsorship placement as judged by Sponsor in its discretion, and not to run-of-site banner advertisements or other rotating promotional placements.

Comment: Exclusivity by a major sponsor is a major concession and often is accompanied by up-front payments or preferential allocation of revenues. Here, the exclusivity is being granted by the website operator, which is typical in response to a major brand's concern not to invest time and resources into a co-branded site only to find competition "in its own backyard."

2.8. WEBSITE OPERATOR USER DATA. Website Operator shall distribute marketing messages on behalf of Sponsor to Website Operator's end users via electronic mail and other methods of communication as mutually agreed by the parties. Furthermore, Website Operator shall make available to Sponsor necessary end user data as reasonably appropriate for marketing. Sponsor acknowledges that all such end user data that is generated by Website Operator is valuable proprietary information of Website Operator, and Sponsor agrees that any use of such end user data shall be limited solely to use for purposes of delivering values to Website Operator end users and for no other purpose. Furthermore, Sponsor acknowledges that any use of Website Operator end user data shall be limited to the extent allowed by and subject to Website Operator's agreement with such end users; provided, however, that Website Operator represents and warrants that such agreements with its end users will not increase Sponsor's duties or decrease its rights, nor reduce Website Operator's obligations to Sponsor under this Agreement, without Sponsor's prior written consent.

Comment: In this sample agreement, the website operator owns all customer data. Care should be taken to ascertain what customer data, if any, may be shared with the sponsor under state, federal, and foreign applicable laws and under the privacy policies and terms of use of the applicable web pages.

3. COMPENSATION AND REPORTING

3.1. UP-FRONT PAYMENT. On execution of this Agreement, Sponsor shall pay Website Operator the amounts set forth on Exhibit A as the "Up-Front Fee" in consideration of Website Operator's development and integration of content for use on the Co-Branded Pages and the Sponsor Website.

3.2. QUARTERLY FEE PAYMENTS. Sponsor shall pay Website Operator the quarterly fees as set forth on Exhibit A attached hereto.

3.3. LAUNCH OF CO-BRANDED PAGES. After execution of this Agreement, the parties shall work together cooperatively to develop a mutually agreeable timeline for the launch of the Co-Branded Pages. If the parties decide that an adjustment to the timing of quarterly payments hereunder is appropriate, the parties may amend the quarterly payment schedule set forth on Exhibit A with a written amendment signed by both parties.

4. TERM AND TERMINATION

4.1. TERM. The Term shall commence on the date of this Agreement and, unless earlier terminated or extended as provided below, shall continue until _ _[*expiration date*]_ _.

4.2. TERMINATION. Either party may terminate this Agreement, effective immediately on written notice to the other party, if the other party should fail to perform any material obligation under this Agreement or cure any other material breach of this Agreement within 30 days after receiving written notice of such nonperformance or breach from the terminating party. In addition, either party may terminate the Term immediately on written notice if the other party shall fail to do business in the normal course or become subject to any bankruptcy, assignment for creditors, corporate dissolution, or similar proceeding.

4.3. EFFECT OF TERMINATION. On termination or expiration of the Term for any reason, all rights and obligations of the parties under this Agreement shall be extinguished, except that the rights and obligations of the parties under Sections 5, 6, 7, and 8 of this Agreement, along with all accrued payment obligations of Sponsor (*i.e.,* the up-front payment referenced in Section 3.1 and set forth in Exhibit A attached hereto), shall survive any termination or expiration of the Term.

5. REPRESENTATIONS AND WARRANTIES; INDEMNITY

5.1. WEBSITE OPERATOR'S REPRESENTATIONS AND WARRANTIES. Website Operator represents and warrants to Sponsor that:

(a) It has full power and authority to enter into this Agreement;

(b) The execution, delivery, and performance by Website Operator of this Agreement will not violate any law, statute, or other governmental regulation, and will not violate any other agreement or instrument to which Website Operator is a party; and

(c) The use of the Website Operator Content will not violate or infringe any Intellectual Property Right or other right of any third party.

5.2. SPONSOR'S REPRESENTATIONS AND WARRANTIES. Sponsor represents and warrants to Website Operator that:

(a) It has full power and authority to enter into this Agreement;

(b) Neither the execution, delivery, and performance by Sponsor of this Agreement, nor the performance of ticketing services by Sponsor, in connection with the Co-Branded Pages, will violate any law, statute, or other governmental regulation or any other agreement or instrument to which Sponsor is a party; and

(c) The use of the Sponsor Content will not violate or infringe any Intellectual Property Right or other right of any third party.

5.3. INDEMNITY. Each party (the "Indemnifying Party") shall indemnify, defend, and hold harmless the other party, its directors, shareholders, officers, agents, employees, successors, and assigns from and against any and all liabilities, obligations, costs, losses, or expenses of whatever kind or nature (including without

limitation reasonable attorney fees and expenses and other litigation expenses), arising from, in connection with, or related in any way, directly or indirectly, to any negligent act or omission by the Indemnifying Party, or to any breach by the Indemnifying Party of this Agreement or of its representations or warranties under this Agreement.

6. EXCLUSIONS; NO LIABILITY

6.1. WARRANTIES EXCLUDED. NEITHER PARTY MAKES ANY OTHER REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, IN CONNECTION WITH THIS AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, (A) WEBSITE OPERATOR MAKES NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE WEBSITE OPERATOR WEBSITE, WEBSITE OPERATOR BRAND FEATURES, OR ANY OTHER ITEMS OR SERVICES PROVIDED BY WEBSITE OPERATOR, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY ARISING BY USAGE OF TRADE, COURSE OF DEALING, OR COURSE OF PERFORMANCE, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND ANY IMPLIED WARRANTY OF NONINFRINGEMENT; (B) SPONSOR ACKNOWLEDGES THAT THE WEBSITE OPERATOR WEBSITE (INCLUDING ANY SERVERS OR OTHER HARDWARE, SOFTWARE, AND ANY OTHER ITEMS USED OR PROVIDED BY WEBSITE OPERATOR IN CONNECTION WITH THE WEBSITE OPERATOR WEBSITE) AND WEBSITE OPERATOR BRAND FEATURES ARE PROVIDED "AS IS" AND THAT WEBSITE OPERATOR MAKES NO WARRANTY THAT THE WEBSITE OPERATOR WEBSITE WILL BE FREE FROM BUGS, FAULTS, DEFECTS, OR ERRORS OR THAT ACCESS TO THE WEBSITE OPERATOR WEBSITE WILL BE UNINTERRUPTED; (C) SPONSOR MAKES NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE SPONSOR WEBSITE, SPONSOR BRAND FEATURES, OR ANY OTHER ITEMS OR SERVICES PROVIDED BY SPONSOR, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY ARISING BY USAGE OF TRADE, COURSE OF DEALING, OR COURSE OF PERFORMANCE, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND ANY IMPLIED WARRANTY OF NONINFRINGEMENT; AND (D) WEBSITE OPERATOR ACKNOWLEDGES THAT THE SPONSOR WEBSITE (INCLUDING ANY SERVERS OR OTHER HARDWARE, SOFTWARE, AND ANY OTHER ITEMS USED OR PROVIDED BY SPONSOR IN CONNECTION WITH THE SPONSOR WEBSITE) AND SPONSOR BRAND FEATURES ARE PROVIDED "AS IS" AND THAT SPONSOR MAKES NO WARRANTY THAT THE SPONSOR WEBSITE WILL BE FREE FROM BUGS, FAULTS, DEFECTS, OR ERRORS OR THAT ACCESS TO THE SPONSOR WEBSITE WILL BE UNINTERRUPTED.

6.2. LIMITATION OF LIABILITY. NEITHER PARTY SHALL HAVE ANY LIABILITY FOR, AND EACH PARTY HEREBY WAIVES AND DISCLAIMS, ANY AND ALL CLAIMS AND CAUSES OF ACTION AGAINST THE OTHER PARTY, WHETHER IN CONTRACT, TORT (INCLUDING, WITHOUT LIMITATION, NEGLIGENCE AND STRICT LIABILITY), WARRANTY, OR OTHERWISE, RELATING TO ANY INDIRECT, CONSEQUENTIAL, OR EXEMPLARY DAMAGES, IN EACH CASE, ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT (INCLUDING ANY BREACH HEREOF) OR ANY OF THE TRANSACTIONS CONTEMPLATED HEREBY.

7. OWNERSHIP

7.1. SPONSOR. As between the parties, Sponsor retains all right, title, and interest in and to the Sponsor Website, the Sponsor Content, and the Sponsor Marks and other Sponsor Brand Features, along with all Intellectual Property Rights associated with any of the foregoing.

7.2. WEBSITE OPERATOR. As between the parties, Website Operator retains all right, title, and interest in and to (a) the Website Operator Content, Website Operator Website (including, without limitation, any and all Website Operator Website Content (other than the Sponsor Content), Sponsor-generated data, URLs, domain names, technology, hardware, software, code, know-how, techniques, algorithms, processes, user interfaces, "look and feel," Trademarks, and any other items posted thereon or used in connection or associated therewith), and the Website Operator Marks and other Website Operator Brand Features, along with all Intellectual Property Rights associated with any of the foregoing.

7.3. OTHER TRADEMARKS. Website Operator shall not register or attempt to register any of the Sponsor Marks or any Trademarks that Sponsor reasonably deems to be confusingly similar to any of the Sponsor Marks. Sponsor shall not register or attempt to register any of the Website Operator Marks or any Trademarks that Website Operator reasonably deems to be confusingly similar to any of the Website Operator Marks.

7.4. FURTHER ASSURANCES. Each party shall take, at the other party's expense, such action (including, without limitation, execution of affidavits or other documents) as the other party may reasonably request to

effect, perfect, or confirm such other party's ownership interests and other rights as set forth above in this Section 7.

8. GENERAL PROVISIONS

8.1. CONFIDENTIALITY. During the Term, and for a period of 5 years thereafter, the receiving party shall not disclose to others or use for any purpose of its own, other than in performance of this Agreement, any Confidential Information of the other party. Each party shall take, at a minimum, measures consistent with those taken to protect its own similar types of Confidential Information (and in any event, at least reasonable measures) to protect the other's Confidential Information against disclosures prohibited by this Agreement. Each party acknowledges that its breach of the provisions of this Section 8.1 will result in immediate and irreparable harm to the other and that money damages alone would be inadequate to compensate such party. Therefore, in the event of a breach of this Section 8.1 by either party, the other party may, in addition to other remedies, immediately obtain and enforce injunctive relief prohibiting the breach or threatened breach or compelling specific performance. Notwithstanding any other provision of this Agreement, the restrictions set forth in this Section 8.1 shall not apply to any information that (a) is in or enters the public domain through no fault of the receiving party; (b) is disclosed to the receiving party by a third party legally entitled to make such disclosure; (c) is independently developed by the receiving party without reference to any Confidential Information of the other party; or (d) is required to be disclosed by applicable law, regulation, or order of any governmental authority; provided that in such event, the receiving party shall provide the disclosing party with prior notice that is reasonable in the circumstances of such disclosure and shall use reasonable efforts to cooperate with the disclosing party to minimize the extent and scope of such disclosure.

Comment: Consider entering into a separate, more complete nondisclosure agreement on a form attached to the contract as an exhibit. See §§4.20-4.21 for a sample form that could be modified for this purpose.

8.2. INDEPENDENT CONTRACTORS. Sponsor and Website Operator are independent contractors under this Agreement, and nothing herein shall be construed to create a partnership, joint venture, franchise, or agency relationship between Sponsor and Website Operator. Neither party has any authority to enter into agreements of any kind on behalf of the other party.

8.3. ASSIGNMENT. Neither party may assign this Agreement or any of its rights or delegate any of its duties under this Agreement without the prior written consent of the other party, not to be unreasonably withheld; except that either party may, without the other party's consent, assign this Agreement or any of its rights or delegate any of its duties under this Agreement (a) to any corporate affiliate of such party; or (b) to any purchaser of all or substantially all of such party's assets or to any successor by way of merger, consolidation, or similar transaction. Subject to the foregoing, this Agreement shall be binding on, enforceable by, and inure to the benefit of the parties and their respective successors and assigns.

Comment: In co-branding relationships, parties often choose their partners based not only on skill sets but also on competitive issues. For example, to preserve the value of proprietary competitive information, many sponsors refrain from working with partners who actively are engaged in cross-marketing activities with a sponsor's competition. Consider carefully the circumstances under which either party will be permitted to assign its rights or subcontract its obligations under this agreement.

8.4. CHOICE OF LAW; FORUM SELECTION. This Agreement shall be governed by, and construed in accordance with, the laws of the State of California without reference to its choice of law rules. Sponsor hereby irrevocably consents to personal jurisdiction and venue in the state and federal courts located in _ _[*city or county*]_ _ California with respect to any actions, claims, or proceedings arising out of or in connection with this Agreement.

8.5. NONWAIVER. No waiver of any breach of any provision of this Agreement shall constitute a waiver of any prior, concurrent, or subsequent breach of the same or any other provisions hereof, and no waiver shall be effective unless made in writing and signed by an authorized representative of the waiving party.

8.6. FORCE MAJEURE. Neither party shall be deemed to be in default of or to have breached any provision of this Agreement as a result of any delay, failure in performance, or interruption of service resulting directly or indirectly from acts of God, acts of civil or military authorities, civil disturbances, wars, strikes, or other labor disputes, fires, transportation contingencies, interruptions in telecommunications or Internet services or network provider services, other catastrophes, or any other occurrences that are beyond such party's

reasonable control.

Comment: Consider carefully what risks that might otherwise be deemed "force majeure" actually should be borne by one of the parties. If one of the alliance parties is a telecommunications carrier, failure of their service should not be deemed to be a force majeure despite the fact that such a failure might be deemed to be a force majeure for another party under other circumstances.

8.7. NOTICES. Any notice or other communication required or permitted to be given under this Agreement shall be given in writing and delivered by first class U.S. mail, in person, or mailed via confirmed facsimile or e-mail, or delivered by courier service, properly addressed and with the required postage or delivery charges prepaid, to the person signing this agreement on behalf of the applicable party at its address specified in the opening paragraph of this Agreement and shall be deemed effective on receipt. Either party may from time to time change the person to receive notices or its address by giving the other party notice of the change in accordance with this section.

8.8. INTEGRATION. This Agreement contains the entire understanding of the parties hereto with respect to the transactions and matters contemplated hereby, supersedes all previous agreements or negotiations between Website Operator and Sponsor concerning the subject matter hereof, and cannot be amended except by a writing signed by both parties. If any provision of this Agreement shall be adjudged by any court of competent jurisdiction to be unenforceable or invalid, that provision shall be limited or eliminated to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect and enforceable.

IN WITNESS WHEREOF, the parties have duly executed and delivered this Agreement as of the date set forth above.

Website Operator

Date: _ _ _ _ _ _

_ _[*NAME OF WEBSITE OPERATOR*]_ _,
a _ _[*state of incorporation*]_ _ **corporation**

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

Sponsor

Date: _ _ _ _ _ _

_ _[*NAME OF SPONSOR*]_ _,
a _ _[*state of incorporation*]_ _ **corporation**

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

EXHIBIT A

PAYMENTS AND EXCLUSIVITY

Comment: Payment and revenue sharing structures in co-branding agreements can be very flexible, and may take the form of up-front payments to fund development or provide an incentive to enter into the transaction, royalties from commercial activities, revenue sharing, or hourly rates for specified services such as customer support provided by one party. The following example includes up-front payments and quarterly fees paid by the sponsor.

1. The Exclusive Categor_ _[*y is:/ies are:*]_ _ _ _[*describe qualifying products or services*]_ _.

2. The up-front payment called for by Section 3.1 shall be _ _[*dollar amount*]_ _.

3. Sponsor shall pay the following non-accrued obligation quarterly fees on or before the following dates:

_ _[*date*]_ _ _ _[*dollar amount*]_ _

_ _[*date*]_ _ _ _[*dollar amount*]_ _

_ _[*date*]_ _ _ _[*dollar amount*]_ _

_ _[*date*]_ _ _ _[*dollar amount*]_ _

EXHIBIT B

TRADEMARKS

The following Trademarks of Sponsor, as well as any additional Trademarks of Sponsor added at a later date, are "Sponsor Marks" as that term is used in this Agreement:
_ _[*depict Sponsor's trademarks*]_ _

The following Trademarks of Website Operator are "Website Operator Marks" as that term is used in this Agreement:
_ _[*depict Website Operator's trademarks*]_ _

EXHIBIT C

SPECIFICATIONS OF CONTENT AND CO-BRANDED PAGES

WEBSITE OPERATOR CONTENT

The following content shall be developed by Website Operator (with input from Sponsor) and provided to Sponsor for inclusion on the Sponsor Website: _ _[*describe Sponsor Website content*]_ _

SPONSOR CONTENT

The following content shall be developed by Sponsor (with input from Website Operator) and provided to Website Operator for inclusion on the Co-Branded Pages: _ _[*describe Co-Branded Pages content*]_ _

EXHIBIT D

SPONSOR PROMOTIONAL ACTIVITIES

Comment: This exhibit lists sponsor's promotional activities in support of the venture and contains examples of types of contributions, such as inclusion in existing web pages, links, logos, and advertising placements.

Sponsor and Website Operator shall work together to develop mutually acceptable content for inclusion in the Website Operator Website.

On each page of the Sponsor Website linked to or from the Co-Branded Pages or containing any Website Operator Content, Sponsor shall include, in a mutually acceptable "above-the-fold" location (based on a 640 × 480 pixels screen), a logo link containing the Website Operator Brand Features, to be supplied by Website Operator, which links back to the Website Operator Website.

Sponsor shall make available to Website Operator _ _[*dollar amount*]_ _ **of advertising placements (based on Sponsor's standard prices for the same or similar advertising) during each of the calendar years** _ _[*year*]_ _ **and** _ _[*year*]_ _ **in marketing vehicles owned or controlled by Sponsor as reasonably requested by Website Operator for the purpose of marketing the Co-Branded Pages and the services provided on such pages. Website Operator acknowledges that marketing pieces included in Sponsor's marketing vehicles must be reasonably consistent with the overall message delivered by such vehicle.**

© The Regents of the University of California

12

Software License Agreements

I. INTRODUCTION §12.1

II. KEY ISSUES IN SOFTWARE LICENSING
- A. Exclusive Licenses §12.2
- B. Nonexclusive Licenses §12.3
- C. Scope of License
  - 1. Scope of Rights Granted §12.4
  - 2. Number of End Users §12.4A
- D. Payment Structures §12.5

III. SAMPLE SOFTWARE LICENSE AGREEMENT
- A. Introduction §12.6
- B. Form: Software License Agreement §12.7

IV. DRAFTING EXCLUSIVE LICENSES
- A. General Considerations
  - 1. Restrictions on Scope or Field of Use §12.8
  - 2. Performance Milestones; Minimum Royalties §12.9
- B. Form: Exclusivity Clause §12.10

V. BANKRUPTCY CONSIDERATIONS
- A. Introduction §12.11
- B. Executory Contracts and Bankruptcy Code §365(n) §12.12
- C. Drafting Considerations §12.13

© The Regents of the University of California

§12.1 I. INTRODUCTION

The functionality of an Internet site is driven by software. A website operator typically licenses software from third parties to operate its site, and may need to sublicense rights to end users of the website so that the end users will be able to fully utilize the site. The Internet is also increasingly being used as a mechanism for software download and distribution; these activities are performed under a distribution license from the software owner. Further, the Internet is becoming a vehicle for creative relationships between companies, coupling software and other resources to create alliances that require joint licenses to effect their purpose.

There are two basic forms of acquisition of rights to use software. The first is a purchase of the code itself, which vests complete ownership in the purchaser. For a software vendor seeking to commercially exploit its products, this model can be limiting, because it does not permit broader-based distribution of the product. The second form of acquisition of rights to software is by license. A software license is a contract granting the licensee certain rights to use the code; ownership, however, is retained by the licensor. The license structure is very flexible, allowing the parties to structure broad or limited scope licenses to suit their objectives.

Sections 12.2-12.7 provide a sample form software license agreement and an analysis of its basic terms from the viewpoints of the licensor and the licensee. This basic license may be coupled with other elements such as software development (see chap 13), a source code escrow (see chap 15), and training, maintenance, and hosting services (see chap 6). Sections 12.8-12.10 discuss certain drafting considerations in preparation of exclusive licenses. Sections 12.11-12.13 review the impact of the bankruptcy laws on software licenses and discuss how to draft licenses to address these issues.

NOTE: Counsel preparing software license agreements and other software contracts for use in an online environment should be familiar with the electronic contracting issues discussed in chap 7. In particular, counsel should be aware of the American Law Institute's Principles of the Law of Software Contracts, approved March 16, 2009. See §7.12.

© The Regents of the University of California

II. KEY ISSUES IN SOFTWARE LICENSING

§12.2 A. Exclusive Licenses

Licenses can be granted on an exclusive or a nonexclusive basis. An exclusive license means that the licensee is the only party permitted to exercise the rights granted by the license. Once an exclusive license is granted, the licensor can grant no further licenses and can itself no longer exercise the rights granted. Exclusive licenses can be limited to certain markets (so that the licensee has exclusivity in a certain geographic market or a specific industry) or to specified types of uses (so that the licensee has exclusive rights, *e.g.,* to train others in the software or to act as a distributor or an installer). See §12.8. Given the worldwide nature of the Internet, geographic limitations are rarely used in connection with Internet-based software.

When are exclusive licenses used? Licensees who are funding development of specialized software often argue for exclusivity as a way of keeping their competition from accessing innovations or improvements to the licensor's base code that the licensee has paid to develop. Exclusivity is used in this context as a means of protecting competitive advantage. In other situations, licensees are performing functions for the licensor, such as software distribution or end user support and training services, and may require exclusivity as a condition of their willingness to invest time and resources in building the business. Exclusivity is often used as an inducement to obtain these services from the licensees. In the context of an online business, exclusive licenses may be appropriate in connection with distribution, if the licensee wishes to be the sole source for products or services distributed online.

An exclusive license can be a very valuable right for a licensee, often meriting significantly higher royalty fees. Granting licenses on an exclusive basis is risky for the licensor, however. In an exclusive license, the licensor limits its opportunity to derive revenue from the subject matter of the license to only one source.

What if the licensee fails to perform? When a licensor grants an exclusive license, it is effectively "putting all its eggs in one basket." If the licensee is not successful, or if the licensee abandons the licensed technology in favor of another project, the licensor will be without revenue and unable to relicense to a third party for the term of the license. A licensor who enters into a long-term exclusive license should therefore consider incorporating into the license structure mechanisms to protect against such risks. Exclusive licenses often include performance milestones such as revenue targets, which, if not met, trigger either the loss of exclusivity or the loss of the license. See §12.9.

Consideration for exclusive licenses may take the form of an up-front payment, a royalty payable over the term of the license, or both. See §12.5. Sections 12.8-12.10 discuss certain drafting considerations for exclusive licenses.

© The Regents of the University of California

§12.3 B. Nonexclusive Licenses

Nonexclusive licenses allow the licensor to grant the same or similar rights over and over again to as many different parties as the licensor chooses. The nonexclusive license is the vehicle for software distribution. A licensor grants each of its end users a nonexclusive license to install and use its software product and can do so for an unlimited number of end users. A classic form of nonexclusive license is the "shrink-wrap" license that accompanies commercial off-the-shelf software, discussed in §§7.2-7.4. The consideration for a nonexclusive license of widely distributed software is typically a single up-front payment. See §12.5.

© The Regents of the University of California

C. Scope of License

§12.4 1. Scope of Rights Granted

The scope of rights to be granted in a nonexclusive software license is an important consideration. It is not always necessary to grant licensees all of the owner's rights to use and exploit the software. For example, an end user may not need the right to modify the software or to copy and distribute it to third parties commercially. Those additional rights may be more valuable and should come with a higher price and a different payment structure, such as a royalty.

When representing a licensee, consider whether the following rights should be granted in order for the licensee to achieve its objectives:

- Reproduction (making copies).
- Distribution or reselling.
- Public display.
- Making modifications or improvements.
- Creation of derivative works.
- Using the license on behalf of others (not merely for the licensee's own internal use), such as in the capacity of a service bureau.
- Hosting the software for third parties.
- Rights to the source code of the software (typically necessary to make modifications).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/12 Software License Agreements/§12.4A 2. Number of End Users

§12.4A 2. Number of End Users

Often, an important element in determining the scope of a software license is the number of end users who will be able to access and use the software. Various structures are commonly used to address this issue. Although vendors have tended to develop their own terminology for their licensing structures, and the same terms may mean different things to different vendors, examples of common structures include the following:

- **Named user license.** Under this structure, each individual user is specifically listed in the license agreement and the license permits use only by the persons named. If an organization with 500 employees desires to license a software product under the named user license method for use by its employees, the license would refer to each of the 500 employees by name and be limited to use by those named individuals. This approach can have negative consequences, however: If provision is not made for swapping out a user who leaves the company, a new license for the user's replacement would have to be purchased.
- **Per seat license.** This structure provides a license for a specified number of end users, or "seats," but actual users are not named. Therefore, if a 500-employee organization desires to license software for use by all of its employees, it would purchase a 500-seat license and cover its needs.

PRACTICE TIP: In negotiating a per seat license, counsel should consider making provision for additional seats at a pre-negotiated price so that negotiations do not need to be reopened each time a new employee joins the organization.

- **Maximum concurrent use license.** If end users will use the software occasionally, not continuously, to do their jobs, the software may be a candidate for a concurrent use license. Under this structure, the parties agree on a maximum number of users who can access the software program at the same time. Monitoring software, either internal or external to the software program, serves as a gatekeeper so that when the maximum user count is reached, additional users are not permitted access to the program until space is available. If an organization with 500 users estimates that only 20 percent of its employees will be using the software at any given time, it can set a 100 maximum concurrent user threshold. If 100 users are using the program, then the 101st user would be required to wait until a user is finished and logs off before he can use the software. This structure can result in cost savings because fewer licenses may be needed to achieve the same operational result.
- **Site license.** Here a license is granted with respect to a specific geographic location or building, usually in the context of an organization that has multiple locations. Sometimes a site license applies to all users located at the site, but more often a maximum capped number of users applies.
- **Enterprise license.** An enterprise license is used where an organization consists of one or more related entities, perhaps at multiple sites, and wants to be able to spread its licensed users across all locations within the organization. Sometimes enterprise licenses apply to all users within an enterprise, but more often a maximum capped number of users applies.
- **Per machine license.** Typically used for software used to administrate and maintain servers and other equipment, this structure assigns the license to a specific computing device whose serial number or other identifying information is listed in the license.

Courts tend to interpret these license scoping provisions narrowly. In *Wall Data Inc. v Los Angeles County Sheriff's Dep't* (9th Cir 2006) 447 F3d 769, the U.S. Court of Appeals for the Ninth Circuit ruled that making and installing copies of software in excess of the number of copies permitted under the applicable license constitutes copyright infringement. In *Wall Data*, the L.A. County Sheriff's Department, preparing for the opening of a new jail, purchased approximately 3700 licenses to Wall Data's software. In order to expedite the rollout of the new computers needed for the jail, rather than manually installing programs onto the computers, the department created a "master" hard drive configuration and used a hard disk imaging methodology to rapidly copy the master configuration onto all of its computers. Ultimately, it installed the Wall Data software on approximately 6000 of its computers. The department claimed that it limited the

number of users who could access and use the software to the number of authorized licenses it had purchased. Rejecting the department's fair use and other arguments, the court found that the making of the unauthorized copies constituted an infringement of Wall Data's copyright.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/12 Software License Agreements/§12.5 D. Payment Structures

§12.5 D. Payment Structures

There are a variety of possible structures for payments due to the licensor under a license agreement. One type of payment is a license fee, a flat amount normally payable up front at the commencement of a license, on renewal, or both. License fees may also be payable in installments over time. License fees are generally viewed as consideration for entering into the license. If the license is an end-user license, use fees can be structured either on a flat-fee basis (*e.g.,* one amount covering an entire business unit up to a maximum number of users or a maximum number of computers accessing the software) or on a per-user or per-computer basis.

If the license is for distribution or resale of a product, royalty payments are typically required. A royalty is usually expressed as a percentage of the licensee's gross or net revenues, based on past sales, and is payable periodically. One area for negotiation in reaching agreement on a royalty structure is the calculation of the royalty base, *i.e.,* the base amount to which the royalty percentage is applied. The licensee's gross revenues from sales of the software may serve as the royalty base, but the licensor must consider whether gross revenues include items such as sales taxes on which a royalty should not be paid. Further, the licensee's gross sales figures may not reflect returns, which are normally deducted from the royalty base. Another approach is to calculate the royalty based on the licensee's net profits from sales of the software. This approach is not as widely used by licensors because it often involves internal overhead charges (*e.g.*, for administrative services and staffing) that are subject to possible abuse by the licensee. It is possible to mitigate these concerns by imposing caps on the allowable charges for administrative overhead. Lower royalty percentages based on gross sales figures are more common, however.

© The Regents of the University of California

III. SAMPLE SOFTWARE LICENSE AGREEMENT

§12.6 A. Introduction

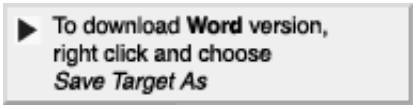
The sample software license agreement in §12.7 contemplates that the licensee will use the code for its internal purposes and also distribute the code to sublicensees. The license is nonexclusive and royalty-bearing, and the licensee is not permitted to make any modifications to the software. For a sample software end-user license intended to be accessed online, see §8.5. Special considerations in drafting exclusive licenses are discussed in §§12.8-12.10.

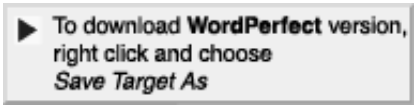
PRACTICE TIP: Every time a document is created in Microsoft Word or Corel WordPerfect, it probably contains "metadata." Metadata are data created about a document, either automatically by the word processing system or manually through embedded data such as comments. Some of this information may be confidential, pertaining to the client for whom counsel is performing the work or to another client whose preexisting document was repurposed as a template for a current project. Because this type of information travels with the document every time it is copied or e-mailed to others, sensitive or confidential information may be inadvertently transmitted via the metadata sent with the document. Therefore, counsel should take care to remove all comments, revision marks, and hidden text that may be embedded in the document, as well as information about prior versions, to review the document's "properties" (found under the "file" pull-down menu), and to remove all sensitive data. See Microsoft's suggestions on identifying and removing metadata at http://office.microsoft.com/en-us/help/HA010776461033.aspx. See chap 20A on the issue of preserving metadata.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/12 Software License Agreements/§12.7 B. Form: Software License Agreement

§12.7 B. Form: Software License Agreement





SOFTWARE LICENSE AGREEMENT

This SOFTWARE LICENSE AGREEMENT (this "Agreement") is entered into between _ _[*name of licensor*]_ _ ("Licensor"), and _ _[*name of licensee*]_ _ located at _ _[*licensee's address*]_ _ ("Licensee"), as of _ _[*date*]_ _ (the "Effective Date"), with reference to the following facts:

Comment: Consider whether entities affiliated with the licensee, such as parent or subsidiary corporations, should be included in the term "Licensee."

A. Licensor is the sole owner of all rights, title, and interest in and to the proprietary software product(s) generally known as _ _[*name of software*]_ _, which is described in further detail in Exhibit A attached hereto and incorporated herein by this reference (the "Licensed Software"), as well as any and all related documentation, user manuals, and related material (collectively, the "Licensed Documentation").

B. Licensee desires to obtain a nonexclusive license to the Licensed Software and the Licensed Documentation so that Licensee will have the right to use and distribute the Licensed Software and Licensed Documentation to third parties in accordance with the terms of this Agreement.

NOW, THEREFORE, in consideration of the terms and conditions set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereby agree as follows:

1. GRANT OF LICENSE. Licensor hereby grants to Licensee for the term of this Agreement a worldwide, nonexclusive license to the object code version of the Licensed Software and the Licensed Documentation, for the following purposes and on the terms and conditions set forth herein:

Comment: This section enumerates the specific rights granted to the licensee. Licensees should pay particular attention to this section and compare the rights they need with the rights granted. License grants should set forth elements such as: (1) the geographic scope of the license (worldwide or otherwise); (2) whether the licensee is limited to use of the code for its internal purposes or is permitted to provide services using the code to others; (3) whether the license is transferable and sublicensable; (4) whether the license is irrevocable and perpetual; and (5) whether the license is exclusive or nonexclusive. Licensees should be aware that no rights beyond those specifically listed are granted. If the licensee determines at a later time that additional rights are needed, the addition of those rights will likely come, if at all, at a price.

(a) USE BY LICENSEE. Licensee may install, use, reproduce, and display the Licensed Software and Licensed Documentation for its internal purposes in support of this Agreement, including, but not limited to, the purposes of internal training of Licensee employees in the use and operation of the Licensed Software.

(b) MARKETING AND DEMONSTRATION. Licensee may display the Licensed Software in order to demonstrate, market, and promote the Licensed Software.

(c) SUBLICENSING AND DISTRIBUTION. Licensee may reproduce, resell, sublicense, and distribute the Licensed Software, the Licensed Documentation, and any alterations thereto, derivative works thereof, or related materials provided by Licensor to Licensee hereunder.

2. OWNERSHIP; RESTRICTIONS. Subject to the rights granted to Licensee under this Agreement, all right, title, and interest in and to the Licensed Software and Licensed Documentation are and shall remain at all times the sole and exclusive property of Licensor. Licensor may use, sell, assign, transfer, and license copies

of and rights in the Licensed Software and Licensed Documentation to third parties in Licensor's discretion free from any claim of Licensee. In addition, Licensee agrees that it shall not, without the express written consent of Licensor, decompile, disassemble, or reverse engineer the Licensed Software, or modify, enhance, or otherwise change or supplement the Licensed Documentation, in whole or in part.

3. PAYMENTS. In consideration of the rights granted hereunder, Licensee shall pay Licensor as follows:

3.1. LICENSE FEES.

(a) For the initial one-year term of this Agreement below, Licensee will pay Licensor _ _[*dollar amount*]_ _ (the "Initial Fee"). Licensee shall pay Licensor 50% of the Initial Fee on the execution of this Agreement, with the remaining 50% of the Initial Fee to be paid upon acceptance by Licensee of the Licensed Software and Licensed Documentation.

(b) For each Renewal Term, Licensee shall pay to Licensor _ _[*dollar amount*]_ _ at least 30 days prior to the commencement of such renewal term (each such payment a "Renewal Fee," and, together with the Initial Fee and any other Renewal Fees, collectively, the "License Fees"). The payment of the Renewal Fee is a condition precedent to the renewal of the Term hereof.

3.2. ROYALTIES.

(a) Licensee shall pay Licensor a royalty of _ _[*number*]_ _% of Adjusted Gross Sales Revenue. Licensee shall pay Licensor a royalty of _ _[*number*]_ _% of revenues received from sublicensees of the Licensed Software and Licensed Documentation.

Comment: If the licensee has the right to sublicense, then there should be two royalty calculations: one for the revenues the licensee receives from direct sales of the software to its own customers, and another for the revenues the licensee may receive from its subdistributors.

(b) "Adjusted Gross Sales Revenue" means all revenues actually received by Licensee from the sale of Products, less only the following specific items related to the manufacture or sale of such Products: discounts; packing, shipping, transportation, and insurance costs; taxes, tariffs, and duties; refunds, returns, or offsets; and sales commissions.

Comment: Sometimes the licensed software is bundled with other code or products. As a consequence, a mechanism for calculating the royalty base from the revenues received from this "mixed" product must be included. The following sample language is intended to do so:

Royalties shall be payable to Licensor only to the extent Licensed Software is used in the manufacture of, or incorporated into, the Product. If any third party or Licensee proprietary technology is also incorporated in or used to manufacture a Product ("Mixed Products"), the royalty due hereunder shall be reduced proportionately by assigning the Licensed Technology a percentage of the Product's core technological elements, and by multiplying the Adjusted Gross Sales Revenue by that percentage to determine the base for calculating the royalty due.

(c) Royalties shall be paid quarterly in arrears within 60 days after the end of each calendar quarter. The Licensee's obligation to pay royalties shall survive the expiration or earlier termination of this Agreement.

Comment: If the Licensee will incur significant startup costs that benefit the Licensor, the Licensor should consider deferring the first royalty payment until Licensee has recouped some or all of its startup investment in the project.

(d) Royalty payments shall be accompanied by a report indicating the method and basis of calculation of the payment; provided that Licensee shall be under no obligation to provide customer names or contact information in the royalty report.

Comment: Consider attaching a sample royalty report as an exhibit to the license agreement to clarify in advance the type of reporting that is required.

(e) LATE PAYMENTS. Interest shall accrue on any amount due and payable hereunder and remaining unpaid for more than 30 days (the "Principal Amount") at a rate per annum which shall from day to day be equal to the

lesser of (1) _ _[*number*]_ _% per year, computed on the basis of a year of 360 days and for the actual number of days elapsed (including the first day but excluding the last day) until payment of the Principal Amount, or (2) the maximum rate of interest permitted from day to day under applicable law.

4. LICENSOR RESPONSIBILITIES

4.1. MATERIALS

(a) Licensor shall deliver to Licensee within 15 days after the Effective Date of this Agreement the Licensed Software and the Licensed Documentation in a form suitable for Licensee's reproduction and use under this Agreement. If Licensee has not notified Licensor of any deficiencies in the Licensed Software or the Licensed Documentation within _ _[*number*]_ _ days after delivery, Licensee shall be deemed to have accepted the Licensed Software and the Licensed Documentation for purposes of Section 3 above.

Comment: In a custom software situation, the acceptance process will likely be more involved, with specifically negotiated acceptance testing procedures, allocation of testing responsibility, and procedures for remediation of errors.

(b) Throughout the term of this Agreement, if Licensor makes any alterations, modifications, improvements, or other changes to the Licensed Software or Licensed Documentation (collectively, "Alterations"), Licensor shall promptly deliver to Licensee complete copies of the Licensed Software and Licensed Documentation, as updated or altered, on completion of such Alterations, and in any event no later than the time Licensor commences utilizing the updated or altered Licensed Software or Licensed Documentation in its own operations, or delivers the same to any third party.

Comment: The licensor may desire to limit this clause to exclude any obligation to deliver alterations that were specifically developed for a customer and are not subject to general commercial distribution.

(c) Licensee may produce advertising or marketing materials, brochures, or other literature relating to the Licensed Software. Licensee also may translate into other languages the Licensed Documentation, any Licensor-supplied sales and marketing materials, or any portions thereof. Any such translations and related works shall be the property of Licensee.

Comment: The licensor may desire to amend this clause to provide that the licensor will receive an unrestricted license back, covering all such translated materials. In that case, the licensee may attempt to request partial reimbursement of its translation costs. The licensor should consider whether it will require prior approval of any such advertising or marketing materials. Prior approval may be covered in Section 4.3 below on use of trademarks.

4.2. TRAINING. Licensor shall provide to Licensee within _ _[*number*]_ _ days after the Effective Date technical training for Licensee's employees in the installation and use of the Licensed Software and Licensed Documentation. The training shall take place at Licensee's facility located at _ _[*address*]_ _ and shall comprise _ _[*number*]_ _ full-time days of instructor training. To the extent Licensee requires additional technical training, such training shall be provided at Licensor's customary and reasonable hourly rates. A mutually agreeable date together with a course outline and the permitted number of attendees shall be set forth in a separate letter from Licensor to Licensee. The course outline and all training materials used in connection with such training shall be deemed "Licensed Documentation" hereunder.

4.3. TRADEMARKS. Licensee may use, reproduce and distribute Licensor's trademarks and service marks, if any, in connection with the performance of Licensee's rights and obligations under this Agreement. Any such use or goodwill received therefrom shall accrue to Licensor, who shall remain the sole owner of such trademarks and service marks. Whenever Licensee uses a name, mark, or logo licensed hereunder it shall print or display the following statement: "The _ _[*name, mark, or logo*]_ _ is used solely by permission of _ _[*name of licensor*]_ _," and print a registered trademark symbol or trademark symbol, whichever is appropriate in Licensor's sole discretion. Licensee shall provide Licensor with a copy of all materials bearing Licensor's trademark or service mark. The trademark rights granted by Licensor hereunder are nonassignable. Any attempted transfer or assignment of such limited license shall terminate the license without further action from Licensor. Licensee shall not remove or destroy any proprietary markings placed upon or contained within the Licensed Software or Licensed Documentation. At the expiration or earlier termination of this Agreement, all rights to use Licensor's trademarks and service marks shall cease unless Licensor provides its written approval to each such use.

Comment: Consider whether marketing and other materials prepared by the licensee and bearing the licensor's trademarks should require prior approval of the licensor. Also consider whether the licensor should develop a style guide for licensees to comply with in use of the licensor's trademarks.

5. TITLE. Licensor represents and warrants that it owns all right, title, and interest in and to the Licensed Software and Licensed Documentation. Licensor warrants that the Licensed Software and Licensed Documentation hereby furnished or to be furnished to Licensee do not and shall not infringe upon or violate any patent, copyright, trade secret, or any other proprietary right of any third party. In the event of any claim by any third party, including the third party licensors of Licensor, against Licensee or any Licensee customer ("Customer"), Licensee shall promptly notify Licensor and, notwithstanding any disclaimer or limitation of liability to the contrary, Licensor shall defend such claim, in Licensee's or Customer's name, but at Licensor's sole expense, and shall indemnify Licensee or Customer against any loss, cost, expense (including reasonable attorney fees and costs) or liability arising out of such claim, whether or not such claim is successful.

6. WARRANTY

6.1. EXTENT OF LIABILITY. Licensor warrants that, for a period of _ _[*number*]_ _ days after the date of Licensee's receipt of Licensed Software (the "Warranty Period"), the Licensed Software will conform to the performance standards and specifications set forth in the Licensed Documentation if properly installed and used in the operating environment specified in such Documentation. Licensor does not warrant that the functions contained in the Licensed Software will meet Licensee's requirements or will operate in the combination that Licensee selects for use, or that the operation of the Licensed Software will be uninterrupted or error free, or that all defects in the Licensed Software will be corrected by Licensor. Licensor's responsibility under this warranty shall be limited to correcting the portion of the Licensed Software that fails to perform substantially in accordance with the said specifications or, at the option of Licensor, refunding the applicable license fees in which event Licensee shall return all copies of the Licensed Software and related Documentation. Licensor shall have no liability under the foregoing warranty if (a) Licensee decompiles, reverse engineers, or modifies the Licensed Software without Licensor's prior written consent, (b) Licensee fails to give Licensor written notice of the claimed breach of warranty, or (c) the failure to perform is caused in whole or in part by persons other than Licensor or by products, equipment, or computer programs not furnished by Licensor. EXCEPT AS OTHERWISE SPECIFICALLY PROVIDED IN THIS SECTION 6.1, LICENSOR MAKES NO OTHER WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Comment: The warranty period in Section 6.1 runs from the Licensee's receipt of the software. Consider whether it would be more appropriate for the warranty period to run from acceptance or installation of the software. The Licensee's interest is to have the warranty period run as long as possible. The Licensee may also wish to impose an outside deadline for repair of defective software.

6.2. VIRUSES. Licensor warrants that, to the best of its knowledge, the Licensed Software when physically delivered under this Agreement does not contain programming code or instruction(s) constructed with the ability to damage, interfere with, or otherwise adversely affect computer programs, data files, or hardware (collectively "Viruses"). Licensor also warrants that it has exercised its best efforts to assure that Viruses have not been introduced into the Licensed Software while the Licensed Software was in its possession. Further, Licensor warrants that the Licensed Software shall not contain any disabling code that will activate on a predetermined date or that can be remotely activated by Licensor without Licensee's prior written consent. In the event that it is determined that such a Virus or disabling code exists, Licensor shall, at Licensee's option, immediately replace any portion(s) of the Licensed Software or Licensed Documentation that cannot be corrected or cured within a reasonable period of time or shall immediately reestablish the affected portion(s) of the Licensed Software or Licensed Documentation to be functionally equivalent to their performance prior to the introduction of the Virus or disabling code. Licensor shall further ensure that all Customers promptly obtain copies of any updated materials provided under this Section 6.2. If neither of the foregoing alternatives is reasonably available to Licensor, then Licensee may terminate this Agreement immediately on written notice to Licensor, and Licensor shall refund to Licensee any License Fees paid for the Licensed Software and Licensed Documentation.

7. INDEMNITY

7.1. INTELLECTUAL PROPERTY INDEMNITY. In the event that an action is filed in a court of competent jurisdiction alleging that Licensed Software used within the scope of the License granted hereunder infringes

any copyright, patent, trade secret, or similar proprietary right of any third party ("Infringement Action"), Licensor shall indemnify, defend, and hold Licensee harmless from and against such Infringement Action and any and all costs, damages, penalties, and expenses, including reasonable attorney fees, finally awarded in actions attributable to such claim, provided that (a) Licensee notifies Licensor in writing of the existence of such Infringement Action within 10 days after Licensee receives notice thereof, (b) Licensor has sole control of the defense of such Infringement Action and all related settlement negotiations, and (c) Licensee provides all reasonable assistance and cooperation in such defense. Notwithstanding the foregoing, Licensor shall have no liability on account of any Infringement Action based on (1) the combination, operation, or use of the Licensed Software with equipment, data, or programming not supplied by Licensor or (2) the use of Licensed Software that has been modified or altered without prior written consent of Licensor. Should the Licensed Software become, or in Licensor's opinion be likely to become, the subject of a claim of infringement, Licensor either shall (at Licensor's election) procure for Licensee and its Customers the right to continue to use the Licensed Software, or replace, or otherwise modify, the Licensed Software to make it noninfringing, provided that there is no material change in the functionality of the Licensed Software. The indemnification provided in this Section 7 shall constitute the entire liability of Licensor with respect to an Infringement Action.

7.2. LICENSOR INDEMNIFICATION. Licensee shall indemnify, defend, and hold Licensor harmless from and against any and all demands, claims, or suits by any third party and any and all costs, damages, penalties, and expenses, including reasonable attorney fees, arising out of or in connection with the use of the Licensed Software and Licensed Documentation by Licensee, its employees, agents, or invitees, except to the extent any such demand, claim, or suit arises out of or in connection with Licensor's breach of its obligations hereunder.

7.3. CROSS INDEMNITY. In the event any negligent act or omission of a party or its employees, agents, or representatives causes or results in loss or damage to, or destruction of property of, the other party or third parties, or death or injury to any persons, then such party shall indemnify, defend, and hold the other party harmless from and against any and all claims, actions, damages, demands, liabilities, costs, and expenses, including reasonable attorney fees, resulting therefrom.

7.4. LIMITATION OF LIABILITY. In no event shall Licensor be liable to Licensee or any third party, under this Agreement or through the use of the Licensed Software or Documentation, for any amounts representing loss of profits, loss of data, loss of business, or indirect, consequential, or punitive damages of Licensee or such third party. Except as set forth in Sections 7.1 and 7.3, Licensor's liability in contract, tort, or otherwise for direct damages to Licensee or any third party arising from this Agreement or the use of the Licensed Software shall be limited to credit for the amount of the applicable fees and royalties payable to Licensor under this Agreement.

7.5. SURVIVAL. The provisions of this Section 7 shall survive the expiration or earlier termination of this Agreement.

8. TAXES. All taxes and charges of any kind imposed by any national, federal, state, or local government with respect to the products, services, or other items covered by this Agreement, or sale or use thereof, or measured by the gross receipts to Licensee under this Agreement, shall be collected and paid by Licensee, exclusive of franchise taxes and taxes based on Licensor's income, which shall be paid by Licensor. The provisions of this Section 8 shall survive the expiration or earlier termination of this Agreement.

9. ESCROW OF SOURCE CODE. The parties agree to enter into a standard source code escrow agreement for the Licensed Software ("Escrow Agreement") on reasonably satisfactory terms between themselves and a reputable escrow agent agreed on by the parties. The terms of the Escrow Agreement shall include standard terms of deposit by Licensor, including, but not limited to, a requirement that Licensor must deposit with the escrow agent source code and any other information necessary to maintain and update the Licensed Software and Licensed Documentation. The Escrow Agreement shall also include standard release terms, including, but not limited to, terms for release of the deposited materials upon occurrence of any of the following: (a) Licensor's inability to cure after 30 days a material breach of its obligations under this Agreement; (b) Licensor's ceasing to conduct its operations pertaining to the Licensed Software in the normal course of business; (c) Licensor's legal or equitable insolvency, including, without limitation, failure to meet its obligations as they mature; (d) the bringing by or against Licensor of any proceedings under any bankruptcy or insolvency law; or (e) the appointment or application for appointment of a receiver or the like for Licensor.

Comment: A source code escrow may not be appropriate or economically justifiable in all circumstances. However, if the licensor is a new and unproven business, then an escrow should give the licensee some insurance against

business risks inherent in a new enterprise. Further, if the licensee is undertaking maintenance obligations with its customers or needs to retain the right to continue to modify the software should the licensor no longer be able to do so (see §§12.11-12.13), then an escrow may be warranted. In lieu of the reference to the agreement in Section 9, a source code escrow agreement could be attached as an exhibit to the license agreement to be executed concurrently with the license. For a sample form of source code escrow agreement, see chap 15.

10. TERM AND TERMINATION.

10.1. TERM.

(a) The initial term of this Agreement shall be for a period of _ _[*number*]_ _ years from the Effective Date, unless sooner terminated in accordance with this Section 10.

(b) This Agreement shall automatically renew for successive one-year renewal terms as long as Licensee has paid the Renewal Fee in accordance with Section 3.1 above; provided, however, that through the second one-year renewal term of this Agreement, either party may terminate this Agreement by providing the other party with written notice of cancellation at least 90 days prior to the expiration of the then-current term.

(c) After completion of the second renewal term, this Agreement shall automatically renew for successive one-year renewal terms; provided, however, that either party shall thereafter be entitled to terminate this agreement by providing the other party with written notice of cancellation at least 30 days prior to the expiration of the then-current term.

10.2. TERMINATION FOR MATERIAL BREACH. Either party may terminate this Agreement (without prejudice to Licensee's rights to obtain source code under the Escrow Agreement) in the event that the other party materially breaches any provision of this Agreement, which breach is not cured within 30 days after receipt of written notice from the nonbreaching party describing the breach in detail.

11. EFFECT OF TERMINATION.

11.1. RETURN OF MATERIALS. On any termination of this Agreement that does not cause the release of materials deposited pursuant to the Escrow Agreement, Licensee agrees to return to Licensor within 30 days all copies of the Licensed Software and Licensed Documentation in Licensee's possession, and to erase or otherwise remove all such items from Licensee computers and storage devices. Licensee hereby agrees to assume all responsibility and attendant cost in returning the Licensed Software and Licensed Documentation.

11.2. RIGHTS OF THIRD PARTIES. The parties hereby agree that the rights of third parties, including but not limited to any Customers existing at the date this Agreement terminates, shall not be prejudiced by any termination of this Agreement and the Customer's right to continuing using the Licensed Software and the Licensed Documentation shall continue notwithstanding any such termination.

12. GENERAL PROVISIONS

12.1. AUTHORITY. Each party represents and warrants that it is a legal business entity duly organized and validly existing in good standing under the laws of the jurisdiction of its formation, and that it has full power and authority to enter into and perform this Agreement. Each party also represents and warrants that the person signing this Agreement on its behalf has been properly authorized and empowered to do so.

12.2. NOTICES. All notices under this Agreement shall be given in writing by delivery by a commercially recognized overnight carrier to the addresses set forth on the first page. Either party may from time to time change its address for notification purposes by giving the other prior written notice of the new address and the date upon which it shall become effective.

12.3. REMEDIES. No remedy conferred on Licensee by any of the specific provisions of this Agreement is intended to be exclusive of any other remedy, and each and every remedy shall be cumulative and shall be additional to every other remedy given hereunder or now or hereafter existing at law or in equity or by statute or otherwise. The election of one or more remedies by Licensee shall not constitute a waiver of the right to pursue other available remedies.

12.4. FORCE MAJEURE. If the performance of this Agreement or any obligation hereunder by any party is prevented, restricted, or interfered with by reason of fire or other casualty or accident, acts of God, severe weather conditions, strikes or labor disputes, war or other violence, any law, order, proclamation, regulation, ordinance, demand, or requirement of any governmental agency or any other act or condition whatsoever beyond the reasonable control of such party, the party whose performance is so affected, on giving prompt notice to the other party, shall be excused from such performance. In the event such force majeure condition continues for 90 days, then the party whose performance is not affected by such condition may, at its option and without liability to the other party, terminate this Agreement.

12.5. RELATIONSHIP. The relationship of the parties under this Agreement is one of independent contractors and no agency, partnership, joint venture, or similar relationship is created hereby. Except as specifically authorized, neither party shall have any authority to assume or create obligations on the other party's behalf. Neither party shall take any action that has the effect of creating the appearance of its having such authority.

12.6. WAIVER. The waiver, modification, or failure to insist by Licensee on any of the provisions of this Agreement shall not void, waive, nor modify any of the other provisions nor be construed as a waiver or relinquishment of Licensee's right to performance in the future of any such provision.

12.7. SEVERABILITY. If any provision of this Agreement is declared or found to be illegal, unenforceable, or void by a court of competent jurisdiction, then both parties shall be relieved of all obligations arising under such provision, but only to the extent that such provision is illegal, unenforceable, or void, it being the intent and agreement of the parties that this Agreement shall be deemed amended by modifying such provision to the extent necessary to make it legal and enforceable while preserving its intent or, if that is not possible, by substituting therefor another provision that is legal and enforceable and achieves the same objective. If the remainder of this Agreement shall not be affected by such declaration or finding and is capable of substantial performance, then, each provision not so affected shall be enforced to the extent permitted by law.

12.8. ASSIGNMENT. Licensee may not assign or delegate any or all of its rights, obligations, and duties under this Agreement without the prior written consent of Licensor, which may be withheld in Licensor's sole discretion. Nothing contained in this Agreement, whether express or implied, is intended to confer on any person or entity other than the parties hereto and their successors in interest and permitted assigns, any rights or remedies under or by reason of this Agreement.

Comment: Consider whether this agreement should be assignable by the licensee to a direct or indirect parent, subsidiary, or other affiliate of the licensee without the consent of the licensor.

12.9. SUCCESSORS. This Agreement shall inure to the benefit of and be binding on the heirs, legal representatives, successors, and permitted assigns of the parties.

12.10. HEADINGS. Headings used herein are for reference purposes only and neither limit nor amplify the terms and conditions herein.

12.11. GOVERNING LAW. This Agreement shall be governed by and construed according to the laws of California as such laws are applied to contracts made and to be performed entirely in California, but without reference to California's rules regarding conflicts of laws. All actions under this Agreement shall be brought in a federal or state court of competent jurisdiction in _ _[*city or county*]_ _, California, and in no other jurisdiction.

12.12. SURVIVAL OF CERTAIN PROVISIONS. Termination or expiration of this Agreement for any reason shall not release either party from any liabilities or obligations set forth in this Agreement that (a) the parties have expressly agreed shall survive any such termination or expiration or (b) remain to be performed or by their nature would be intended to be applicable following any such termination or expiration. The provisions of this Section 12 shall survive the expiration or earlier termination of this Agreement.

12.13. ENTIRE AGREEMENT. This Agreement, together with its exhibits, constitutes the entire understanding and agreement between the parties with respect to the subject matter hereof and supersedes any and all prior or contemporaneous oral or written communications with respect hereto, all of which are merged herein. Except as specifically provided for herein, this Agreement may not be altered, amended, or modified except by an instrument in writing signed by a duly authorized representative of each party.

12.14. CONFIDENTIALITY. The parties have executed a separate Non-Disclosure Agreement, a form of which

is attached hereto as Exhibit B, concurrently with the execution of this Agreement and as a condition precedent to the effectiveness hereof.

12.15. MEDIA RELEASES. All media releases, public announcements, and public disclosures by Licensee or its employees or agents related to this Agreement or its subject matter, including, without limitation, promotional or marketing material, but not including any announcement intended solely for internal distribution by Licensee or any disclosure required by legal, accounting, or regulatory requirements beyond the reasonable control of Licensee, shall be coordinated with and approved by Licensor in writing prior to the publication thereof.

12.16. HIRING OF EMPLOYEES. Licensee agrees that, beginning as of the Effective Date, during the term of this Agreement and for a period of _ _[*number*]_ _ years thereafter, neither it nor any of its affiliates shall, except with the prior written consent of the Licensor, offer employment to or employ any person employed then or within the preceding 12 months by Licensor who came in contact with a person who was directly or indirectly involved in the performance of services or provision or receipt of products hereunder.

12.17. COMPLIANCE WITH LAWS. Licensee agrees to comply with all applicable federal, state, and local statutes, ordinances, rules, and regulations, including, without limitation, the rules and regulations under the U.S. Export Administration Act and the U.S. Foreign Corrupt Trade Practices Act, as the same may be amended from time to time. Without in any way limiting the foregoing, (a) Licensee shall not export or otherwise remove any Licensed Software or Licensed Documentation from the United States, either directly or indirectly, without the consent of Licensor and without first obtaining any licenses or approvals as may be required from the U.S. Department of Commerce and any other applicable agency or department of the United States Government, and (b) Licensee agrees that neither it, nor any officer, director, employee, or agent of it (1) shall pay or be instructed to pay or give anything of value, either directly or indirectly, to an official of any foreign government or any foreign political party for the purpose of influencing an act or decision in such person's official capacity, or inducing such person to use such person's influence with the foreign government in order to assist Licensee in obtaining or retaining business for or with, or directing business to, any person, or (2) are at present or shall at any time during the term of this Agreement become an official, officer, or representative of a foreign country.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the Effective Date.

Date: _ _ _ _ _ _

_ _[*NAME OF LICENSEE*]_ _,
a _ _[*state of incorporation*]_ _ **corporation**

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

Date: _ _ _ _ _ _

_ _[*NAME OF LICENSOR*]_ _,
a _ _[*state of incorporation*]_ _ **corporation**

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

© The Regents of the University of California

IV. DRAFTING EXCLUSIVE LICENSES

A. General Considerations

§12.8 1. Restrictions on Scope or Field of Use

When granting an exclusive license of intellectual property or technology, the licensor should consider whether there should be any limitations on the intended scope or field of use of the licensed property. If the licensed technology has multiple nonconflicting applications and the intended licensee is only capable of exploiting one of them, then the scope of the license should perhaps be limited to that particular field of use. For example, software that is capable of determining the shortest route between two points on a map may have multiple applications in the consumer, freight handling, defense, and oil and gas industries. If the licensee's business is the provision of online map generation services targeted at consumers, the licensor should consider limiting the field of use to that specific purpose in order to permit it to relicense the technology on an exclusive basis in other industries.

© The Regents of the University of California

§12.9 2. Performance Milestones; Minimum Royalties

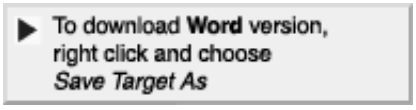
As discussed in §12.2, a licensor who grants an exclusive license essentially puts all its eggs in one basket. Potentially, the licensor risks a total loss of revenue and the inability to relicense if the licensee is unsuccessful or if the licensee abandons the licensed technology in favor of another project. Long-term exclusive licenses should include mechanisms to protect against these risks. One type of protection is the inclusion of performance milestones, by which the parties agree on metrics to indicate that the licensee is properly developing the market for the licensed technology. Many different types of metrics can be used depending on the circumstances. Common examples are the achievement of research and development milestones, minimum sales thresholds, or annual marketing expenditures. Any metric chosen should be objective and easily measurable.

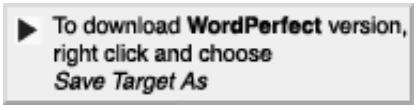
Another type of protection is a minimum guaranteed annual royalty. There are many types of minimum royalty structures that can be used, such as a flat fee per year or an amount that escalates or declines over time. The right approach depends on the applicable market and the circumstances of the license. If annual royalty payments do not reach the minimum level in any period, the license could provide that licensee may choose either to remit payment for the difference or to convert its license to a nonexclusive license. In this way, the licensor is guaranteed a certain level of revenue from its license.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/12 Software License Agreements/§12.10 B. Form: Exclusivity Clause

§12.10 B. Form: Exclusivity Clause





The license rights granted to Licensee hereunder shall be exclusive, provided that Licensee complies with the following requirements (the "Exclusivity Requirements"):

(a) Perform the Performance Milestones attached as Exhibit A on or before the required deadline for each such Performance Milestone as set forth on Exhibit A; and

(b) Pay to Licensor the annual minimum royalty set forth in Exhibit B on or before the due dates set forth in Exhibit B.

If Licensee fails to perform an Exclusivity Requirement when due, Licensor shall provide Licensee with written notice of such failure and 30 days to cure. If such failure is not cured within the 30-day period, the license rights granted herein shall become nonexclusive.

© The Regents of the University of California

V. BANKRUPTCY CONSIDERATIONS

§12.11 A. Introduction

Internet businesses that build infrastructure and systems based on software licensed from third parties benefit from the fact that they avoid incurring research and development costs to create the software. They do, however, bear the risk of dependence on the stability of their licensor and the licensor's business. If the licensor files for bankruptcy, the licensee's Internet business risks losing its investment in the code and incurring the cost of replacing the software or developing a replacement on its own. Sections 12.12-12.13 discuss the implications of bankruptcy on a software license from the licensee's perspective and the protections provided under the Bankruptcy Code (Title 11 USC) for software licensees. This discussion is intended to provide an overview of bankruptcy-related issues in software licensing to assist the practitioner in understanding the risks and benefits available under the Bankruptcy Code and to anticipate those risks and benefits in the license drafting process. If either party to a software license files a bankruptcy case, the other party should seek the advice of experienced bankruptcy counsel.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/12 Software License Agreements/§12.12 B. Executory Contracts and Bankruptcy Code §365(n)

§12.12 B. Executory Contracts and Bankruptcy Code §365(n)

On the filing of a petition for relief under the Bankruptcy Code, "all legal or equitable interests of the debtor [the bankrupt party] in property" become the property of the bankruptcy estate. 11 USC §541(a)(1). If the bankrupt party has an interest in a license of intellectual property, the bankruptcy's interest in the license becomes property of the bankruptcy estate. The bankruptcy trustee (or the debtor in possession, if the case is a Chapter 11 case) may then assume, assume and assign, or reject the license as an executory contract under §365(a) of the Bankruptcy Code. 11 USC §365(a).

The term "executory contract" is not defined in the Bankruptcy Code. The legislative history to §365(a) indicates that a contract should be "executory" when "performance remains due to some extent on both sides." H Rep No. 95-595 at 347 (1977); S Rep No. 95-989 at 58 (1978). Another definition of an "executory contract" often used by courts is the "Countryman" definition (Countryman, *Executory Contracts in Bankruptcy, Part I*, 57 Minn L Rev 439, 446 (1973)):

> [An executory contract is] a contract under which the obligations of both the bankrupt and the other party to the contract are so far unperformed that the failure of either to complete performance would constitute a material breach excusing the performance of the other.

Software licenses are usually classified as executory contracts. Both the licensor and the licensee have obligations that continue until the termination of the license, such as payment, royalty reporting, indemnification, training, and confidentiality. *Fenix Cattle Co. v Silver (In re Select-A-Seat)* (9th Cir 1980) 625 F2d 290, 292. In *Select-A-Seat,* the court held a software license agreement to be executory based partly on the fact that the licensor had a continuing obligation not to license the software to a third party. A mere obligation to make payments is insufficient to render a contract an executory contract under the Bankruptcy Code. Software licenses, however, typically contain covenants, warranties, and other ongoing obligations in addition to the obligation to pay license fees and royalties. *Lubrizol Enters., Inc. v Richmond Metal Finishers, Inc.* (4th Cir 1985) 756 F2d 1043, 1046, cert denied (1986) 475 US 1057.

The debtor-licensor has a choice of "assuming" the license (*i.e.*, keeping it in effect) or "rejecting" the license (*i.e.*, terminating it). To assume a license the licensor must (1) cure, or provide adequate assurance that it will promptly cure, any default; (2) compensate any third party for any pecuniary loss caused by a default; and (3) provide adequate assurance of future performance. 11 USC §365(b)(1). Once assumed, the licensor may either hold the license or assign it to a third party for value. If the licensor rejects the license, the licensee is left with an unsecured claim for breach of contract as if the breach occurred immediately before the bankruptcy filing.

Congress believed it was necessary to provide the licensee of a bankrupt licensor additional protections because of the detrimental effect that rejection of an intellectual property license could have on a licensee's business. Bankruptcy Code §365(n) gives software licensees some protection by allowing licensees to retain their rights in the subject matter of the license (except rights in trademarks and certain other intellectual property) despite the licensor's rejection of the license agreement.

Under 11 USC §365(n), the licensee has two options on the debtor-licensor's rejection of the license agreement. First, if the rejection of the license constitutes a breach that would entitle the licensee to terminate the license agreement, the licensee can elect to treat the license as terminated and then has a damage claim against the licensor. 11 USC §365(n)(1)(A). This option presents difficulties for the licensee. It is often hard to measure monetary damages resulting from the rejection of the license. Moreover, damages are not what the licensee typically wants. The licensee would rather have continued access to the intellectual property it bargained for so that it can continue to use it in its business.

Second, the licensee can elect to retain certain rights under the license as those rights existed immediately prior to the bankruptcy. The rights permitted to be retained, however, are not all of the rights contained in the original license agreement. 11 USC §365(n)(1)(B). The retained rights continue for the duration of the agreement's initial term and any lawful extensions of it. 11 USC §365(n)(1)(B). In return, the licensee must make all royalty payments due under the license for the duration of the license, and must waive any rights of setoff and any administrative claims in the bankruptcy arising from the debtor's nonperformance of the license. Section 365(n)(1)(B) does not provide for the

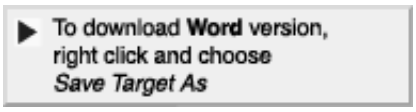
continuation of future performance by the licensor (other than any exclusivity covenants), and the licensee has no rights to the subject intellectual property other than those in existence as of the date of the bankruptcy filing. Therefore, it is arguable that the licensee does not have rights to future modifications or enhancements. S Rep No. 100-505 at 9 (1988).

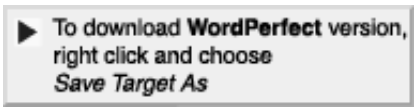
The bankruptcy trustee or debtor-in-possession is usually not required to perform the licensor's obligations under an executory contract pending its decision to assume or reject the contract. This is because the contract is not enforceable against the bankruptcy estate until it has been assumed. *NLRB v Bildisco & Bildisco* (1984) 465 US 513, 532, 79 L Ed 2d 482, 499, 104 S Ct 1188. Section 365(n), however, gives a licensee the right to request that the licensor continue to perform. 11 USC §365(n)(4). Once the licensee makes such a request in writing, the trustee or debtor in possession must either (1) continue to perform the licensor's obligations under the license, or (2) turn over to the licensee the intellectual property subject to the license. 11 USC §365(n)(4)(A).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/12 Software License Agreements/§12.13 C. Drafting Considerations

§12.13 C. Drafting Considerations





Inserting the certain provisions in the licensing agreement may assist the licensee in obtaining the benefits of 11 USC §365(n). The following provision in the license agreement may be helpful:

To the extent this Agreement is determined to be an executory contract under §365 of the Bankruptcy Code (11 USC §365), it is an intellectual property license within the meaning of §365(n) of the Bankruptcy Code.

To provide a clearer path toward termination of the license on rejection by a licensor in bankruptcy, the license agreement should:

- Identify the ongoing obligations of each of the parties to the license and provide that failure to perform them constitutes a material breach of the license.
- Include as an "event of default" the licensor's rejection of the license agreement under 11 USC §365(n).
- Include as an "event of default" the licensor's breach or failure to perform any of its obligations, covenants, or agreements under the license agreement.
- State that the licensee has a right to terminate the license agreement upon the licensor's default.

In addition, the license fee can be structured so that it will be reduced if future improvements are no longer provided. If the debtor-licensor rejects the license and the licensee elects to retain its rights, the licensor will no longer be required to provide improvements and the license fee should be reduced automatically. Further, because it may be hard to value the licensee's damages if a license is terminated, the agreement should include a liquidated damages clause to assist in the determination of monetary damages in a bankruptcy setting if the license is rejected. A significant liquidated damages amount may also serve to discourage the debtor in possession or the trustee from rejecting the contract.

Under 11 USC §365(n), a licensee that retains its rights under the license must continue to make all royalty payments. There is a risk that if the licensor is performing additional services (such as training and maintenance) and the fees for those services are bundled with the license fee, the licensee may end up paying more than it should for the retained license. If the fees are bundled, it may be difficult to argue that the fees should be reduced if the licensor's services are reduced. Therefore, it is advisable to provide for separate fees for each additional service the licensor agrees to perform, so that if certain services will no longer be performed after bankruptcy, payment for those services can easily be segregated and discontinued.

If the license is rejected, the licensee may need to hire third-party vendors to provide support and maintenance services previously furnished by the licensor. The license agreement should permit the licensee to give any such third parties access to and use of the software. To facilitate this type of provision, the licensee should also have access to the source code for the purpose of making modifications and maintaining the software.

NOTE: Certain contract clauses that are triggered by the bankruptcy or insolvency of a party may be unenforceable as so-called ipso facto clauses under Bankruptcy Code §365(e). 11 USC §365(e). That section provides that no rights or obligations under an executory contract may be terminated or modified after a bankruptcy filing solely because of a contract provision that is conditioned on the debtor's bankruptcy, insolvency, or financial condition.

A source code escrow agreement may be used to mitigate the risk that future improvements may no longer be available to the licensee under 11 USC §365(n). For further discussion of source code escrows, see chap 15. Because agreements that are "supplements" to an intellectual property license agreement are covered by §365(n), the escrow agreement should state that it is a supplement to the underlying license agreement.

© The Regents of the University of California

13

Software Development Agreements

I. INTRODUCTION §13.1

II. OWNERSHIP ISSUES §13.2

III. FORM: SOFTWARE DEVELOPMENT AGREEMENT §13.3

IV. SOFTWARE EVALUATION
- A. Introduction §13.4
- B. Form: Software Test and Evaluation Agreement §13.5

© The Regents of the University of California

§13.1 I. INTRODUCTION

Software programs are often created in connection with the construction of an Internet site or the development of back-end systems for data mining, e-commerce, or other website functionalities. These software programs may be created by an external website developer or by a third party. Sections 13.2-13.5 discuss issues that arise in contracting with developers for creation of such software.

A form of software development agreement is provided in §13.3. This type of agreement is entered into between the owner of an e-business website and an independent contractor for the development of software to fit specific needs when the functionality desired is not commercially available. Sections 13.4-13.5 discuss software evaluation agreements, which are entered into with a third party to test the software for "bugs" and other problems before the software is completed and ready for launch.

NOTE: Counsel preparing software-related contracts for use in an online environment should be familiar with the electronic contracting issues discussed in chap 7.

© The Regents of the University of California

§13.2 II. OWNERSHIP ISSUES

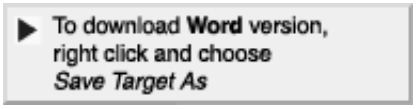
Developers are rarely hired to do custom development work in which software is developed entirely "from scratch" for a customer. Yet even in situations where the developer does not use third party licensed software as a foundation for development of the customer's program, the developer's finished work often contains underlying software or shelf code that the developer owns and uses in its other development projects.

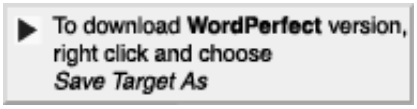
In some cases, a developer takes its own standard "off the shelf" software and simply modifies it or adds new screens to meet a customer's needs. Such developers typically use their own base software to develop products for more than one client. This results in a tension between the customer, who may wish to own the rights to the modifications it pays for, and the developer, who may view some or all of the modifications as extensions of its base software, which it may need to use in future projects. These ownership issues are substantially similar to the ownership issues discussed in §§5.11-5.13 in connection with website development agreements, and must be addressed in the software development agreement.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/13 Software Development Agreements/§13.3 III. FORM: SOFTWARE DEVELOPMENT AGREEMENT

§13.3 III. FORM: SOFTWARE DEVELOPMENT AGREEMENT





SOFTWARE DEVELOPMENT AGREEMENT

This Software Development Agreement (the "Agreement") is entered into as of _ _[*date*]_ _, by and between _ _[*name of company*]_ _, located at _ _[*company's address*]_ _ ("Company"), and _ _[*name of developer*]_ _, located at _ _[*developer's address*]_ _ ("Developer").

NOW THEREFORE, in consideration of the mutual promises made herein and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties agree as follows:

1. SERVICES. Developer will develop software (the "Software") according to the detailed specifications contained in Exhibit A attached to this Agreement (the "Specifications"), technical documentation for the Software in accordance with the Specifications (the "Documentation"), and additional tangible deliverables listed on Exhibit A in accordance with the Specifications (the "Additional Deliverables"). The Software, Specifications, Documentation, and Additional Deliverables are referred to herein collectively as the "Work Product." Developer shall develop the Work Product in accordance with the development schedule set forth in Exhibit B (the "Development Schedule"). Developer must deliver the completed Work Product by the final delivery date specified in Exhibit B (the "Delivery Date"), and Developer agrees to be bound by the Development Schedule. Developer shall develop the Work Product in conformance with standard industry best practices. The acceptance testing process for the Work Product is attached as Exhibit C. Once the Company has accepted the Work Product, the Developer will install the Software on _ _[*describe hardware on which Software will be installed*]_ _. Company will not make final payment to Developer under this Agreement until Company has provided written notice of acceptance in accordance with Exhibit C.

Comment: The development schedule should read as a list of "milestones," *i.e.,* concrete steps in the process of finalizing the project that are measurable and discrete. Each milestone should have a date by which it should be completed. Specifications should be as detailed as possible and should be reviewed by counsel to confirm that they are complete and do not contain any operative provisions that may be at odds with terms in the body of the contract. Consider whether the developer will provide any training or post-delivery consulting services as part of this agreement. If so, the services to be provided at no additional cost should be specified, and an hourly rate should be listed for any additional services the company may request. Also, consider adding a provision that the developer will provide all systems engineering services necessary to develop and install the software, such as programming development, systems analysis and design, conversion and implementation planning, and installation evaluation.

NOTE: If the development of specifications is an obligation to be performed by the developer under this agreement after its execution, the agreement must be modified to add this obligation and to create an exit strategy if the parties are unable to reach agreement on the specifications within a stated period of time. Consider the following language:

Within _ _[*number*]_ _ business days after the date of this Agreement, representatives of the parties shall meet and discuss the basic purpose and functions of the Software and Additional Deliverables and the specific features that the Software will need to contain to accomplish that purpose. Following agreement on the purpose and basic features of the Software and Additional Deliverables, Developer shall prepare draft specifications for the Software and Additional Deliverables

[*If appropriate, add*]

and acceptance testing procedures and criteria.

[*Continue*]

If these draft specifications _ _[*and acceptance testing procedures and criteria*]_ _ are acceptable to Company,

Company shall execute a copy of thereof, which shall then become the Specifications _ _[*and acceptance testing procedures and criteria*]_ _ for purposes of this Agreement. If Developer and Company are unable to agree on specifications _ _[*and acceptance testing procedures and criteria*]_ _ for the Software and Additional Deliverables within such period, this Agreement may be terminated on written notice by either party and all copies of materials furnished by Company to Developer shall be returned immediately.

2. MODIFICATION OF SPECIFICATIONS. Company may make Amendments to the Specifications from time to time by written notice to Developer. In the event of any such amendment to the Specifications, Developer shall notify Company in writing within 10 days of any necessary adjustment to the Fees, and Company shall have the right to withdraw or modify the amendment or, if Company determines to do so in its discretion, terminate this Agreement. If Company exercises such termination right, its sole obligation under this Agreement is to pay Developer any amounts that remain unpaid for services actually rendered up to the date Developer receives written termination notice.

Comment: The company needs the flexibility to change the specifications to address items that it may have forgotten or new requirements that have come to its attention. Any change will necessarily have an impact on the development fees, especially in a fixed price arrangement. The above language provides an exit opportunity for the company if the fee increase resulting from the required change makes the project too expensive.

3. OWNERSHIP OF WORK PRODUCT.

[*Select one of the following alternatives*]

[*Alternative 1: Company will own Work Product developed under Agreement*]

All originals and copies of the Work Product, as well as intermediate versions and working papers and all copyrights, trade secrets, know-how, patents, trademarks, and all other intellectual property rights in the Work Product and all inventions embodied therein (collectively, the "Proprietary Rights") will be the exclusive property of Company and shall constitute trade secrets owned exclusively by Company. Developer hereby assigns and agrees to assign all Proprietary Rights to the Company, for no further consideration, and agrees to require its employees, agents, and independent contractors to assign all Proprietary Rights to Developer in a manner consistent with this Agreement. Developer agrees to assist Company to register, enforce, and maintain any and all Proprietary Rights in any and all countries considered relevant by Company in its discretion. Developer agrees to execute and deliver all documents requested by Company in connection with such registration and enforcement, and to perfect any such rights in Company, its licensees, successors, and assigns. At no time, without the prior written consent of Company, will Developer use, copy, disclose to any third party, license, transfer, or otherwise exploit the Proprietary Rights. Further, Developer will maintain the confidentiality of the fact that Company is pursuing development of the Work Product. Developer will use and maintain appropriate security measures to honor all of such obligations.

[*Alternative 2: Developer will retain ownership of Work Product*]

Company and Developer agree that all original material, including all computer programs and all related printed materials comprising the Work Product, originated and prepared for Company by Developer under this Agreement, shall belong exclusively to and be the property of Developer. Developer agrees, however, that on receipt of payment in full under the terms of this Agreement, Developer shall convey to Company _ _[*a nonexclusive/an exclusive*]_ _ _ _[*assignable/nonassignable*]_ _, perpetual, royalty-free, worldwide license for the use of the Work Product (in object code and source code versions) which _ _[*shall/shall not*]_ _ include the right to reproduce, publish, or sublicense the Software to other parties and _ _[*shall/shall not*]_ _ include the right to make modifications to the Work Product.

Comment: If the developer is paid in full to develop the work product, but then retains ownership of the work product and is able to commercially exploit it through work with third parties, consider whether this result constitutes an unfair "windfall" to the developer. The company may wish to negotiate an agreement by the developer to pay the company a royalty on each license that developer grants with respect to the work product or any modification or amendment it makes to the work product for the benefit of third parties. This royalty could be capped at the cost that the company paid to develop the work product, or it could be some multiple of that cost.

If there is a possibility that the developer may use or integrate material to which third parties hold copyrights or other intellectual property rights, the agreement should state that the developer may not do so unless such use is allowed under the doctrine of "fair use." See §§1.18-1.22. The agreement should also state that the developer will be liable for,

and will hold the company harmless from, any claims of infringement arising from the developer's use or integration of any third party materials in the software developed.

The developer may require that it retain ownership to any tools it develops under the agreement that may have future utility or economic value. If so, the developer may request language similar to the following:

Developer and Company agree that any software or underlying development tools developed or owned by Developer and used by Developer to create or modify the Software shall belong exclusively to Developer.

This is broad language that could be narrowed by describing the particular types of tools to be retained by the developer and including the description in the agreement or in the developer's work plan so that the company does not pay for the tools or pays only part of their development cost. The company should also require the developer to license the tools to the company for the company's own use on a perpetual, royalty-free, worldwide basis.

4. PAYMENT FOR DEVELOPMENT SERVICES.

[*Select one of the following alternatives*]

[*Alternative 1: Payment by hourly rate*]

Company shall pay Developer for all development services rendered in accordance with Developer's established hourly rates contained in its rate schedules dated _ _[*date*]**_ _, which are attached to this Agreement as Exhibit A and incorporated herein by reference, and all applicable taxes, including sales or use taxes. _ _**[*In no event shall the total amount to be paid by Developer hereunder exceed _ _*[*dollar amount*]*_ _ (the "Maximum Amount") without the prior written approval of the Company. If such approval is denied or is not provided within _ _*[*number*]*_ _ days after receipt of written notice from Developer, the parties shall negotiate in good faith for a period of _ _*[*number*]*_ _ days to reach a mutually acceptable adjustment to the Maximum Amount. If they are unable to reach agreement, _ _*[*either party may terminate this Agreement on written notice/either party may submit the matter to binding arbitration pursuant to Section _ _ below*]*_ _]_ _**. Company shall pay Developer's _ _**[*e.g., pre-approved travel costs, including travel time, meals, and lodging, related to performance of this Agreement*]**_ _. Company shall also reimburse Developer for special or unusual expenses incurred at Company's specific written request. Charges shall be billed _ _**[*monthly/on project completion/on acceptance/on completion of milestones in accordance with the schedule attached as Exhibit _ _*]**_ _ and shall be payable within 30 days after Company's receipt of invoice. Final Payment is contingent on completion of the Work Product and its acceptance by Company under Exhibit C.**

[*Alternative 2: Lump sum purchase price*]

Company shall pay Developer the sum of _ _[*dollar amount*]**_ _ as the price for all services rendered on completion of acceptance testing of the Work Product in accordance with Exhibit C. Concurrent with the execution of this Agreement, Company shall deposit with Developer an amount equal to _ _**[*number*]**_ _ percent of that purchase price to be applied against the purchase price.**

5. LIMITED WARRANTY AND LIMITATION OF LIABILITY

5.1. WARRANTY. Developer warrants that the Work Product will perform in accordance with the Specifications for a period of _ _[*e.g., 180 days*]**_ _ from the Delivery Date. If during this time period the Work Product does not perform as warranted, Developer shall, at its option, undertake to correct the Work Product, replace such Work Product free of charge, or, if neither of the foregoing is commercially practicable, refund to Company the fees paid under this Agreement. In addition, Developer warrants that the media on which the Software is distributed will be free from defects in materials and workmanship under normal use for a period of _ _**[*e.g., 30*]**_ _ days from the Delivery Date. Developer will replace any defective media returned to Developer within the _ _**[*e.g., 30-day period*]**_ _. The foregoing are Developer's sole and exclusive remedies for breach of warranty. The warranty set forth above is made to and for the benefit of Company only and will apply only if the Software has been properly installed and used at all times in accordance with the Documentation and no modification, alteration, or addition to the Software has been made, other than those made by Developer or its authorized representatives.**

Comment: For an additional charge, most developers make extended warranty and maintenance packages available to provide ongoing support for the software beyond the standard warranty period. Typically, these services and the corresponding fees are negotiated at the time the development agreement is entered into, to preserve the leverage the

customer has in the negotiations. If the customer opts for these additional services, a separate maintenance and support agreement would be entered into that provides for the specific services the developer would provide, rates and fees, and any service level commitments (such as timeframes for responses to error reporting).

5.2. INFRINGEMENT. Developer represents, warrants, and covenants that the Work Product does not and will not infringe the right, title, and interest of any third party. As of the date of this Agreement, Developer represents and warrants that it has no reason to believe that it will not have sufficient right, title, and interest in the Work Product contemplated to be delivered to prevent its ability to deliver the Work Product without breaching this Section. Developer will defend, indemnify, and hold Company harmless from and against any and all damages, liabilities, costs, and expenses (including but not limited to attorney fees) incurred by Company as a result of any judgment or proceeding against Company or any of its customers in which it is determined or alleged that the Work Product, or any part thereof, infringes any patent, copyright, trademark, trade secret, or other proprietary right of any third party.

5.3. DISCLAIMER. Except as set forth above, Developer makes no warranties, whether express, implied, or statutory, regarding or relating to the Work Product, or any materials or services furnished or provided by Developer under this Agreement, including Maintenance and Support. Developer specifically disclaims all implied warranties of merchantability and fitness for a particular purpose with respect to the Work Product, and with respect to the use or operation of any of the foregoing. In no event will Developer be liable for any loss of profits, loss of use, business interruption, loss of data, cost of cover, or indirect, special, incidental, or consequential damages of any kind in connection with or arising out of the furnishing, performance, or use of the Work Product or services performed under this Agreement, whether alleged as a breach of contract or as tortious conduct, including negligence, even if Developer has been advised of the possibility of such damages.

6. CONFIDENTIAL INFORMATION

6.1. DEFINITION OF CONFIDENTIAL INFORMATION. As used in this Agreement, "Confidential Information" means any information furnished or disclosed, in whatever form or medium, by one party (the "Discloser") to the other party (the "Recipient") relating to the business of the Discloser, that derives independent economic value, actual or potential, from not being generally known to the public and is the subject of efforts that are reasonable under the circumstances to maintain its secrecy. Confidential Information includes, without limitation, contract terms, financial information, customer information, business procedures, processes, techniques, methods, ideas, discoveries, inventions, processes, developments, records, product designs, source code, product planning, trade secrets, and the terms of this Agreement, all of which are deemed confidential and proprietary.

6.2. LIMITATION. Confidential Information does not include any information that Recipient can demonstrate: (a) was publicly available at the time of disclosure, or later became publicly available through no act or omission of Recipient; (b) was already in its possession at the time of disclosure; (c) was rightfully received by Recipient from a third party without any obligation of confidentiality; or (d) was independently developed by or for Recipient without use of Discloser's Confidential Information.

6.3. RESTRICTION ON USE AND DISCLOSURE. Recipient agrees that during the term of this Agreement and for a period of 3 years thereafter, Recipient will regard and preserve such information and materials as strictly confidential, and without the express prior written consent of the Discloser, will not directly or indirectly disclose to any third person, or use for the benefit of anyone other than Discloser, any and all Confidential Information. Recipient may, however, disclose Confidential Information to its officers, employees, and agents who have a need to know such information and who have signed a nondisclosure agreement or otherwise have confidentiality obligations to the Recipient. Recipient agrees that all information, documents, data, and other tangible material pertaining to Confidential Information obtained from or through Discloser shall remain the property of Discloser. Recipient will be responsible for any breach of the confidentiality obligations of its employees and agents.

Comment: This confidentiality provision is mutual and anticipates an exchange of confidential information. If it is more accurate to provide for a "one way" disclosure of confidential information from the company to the developer, this clause should be modified accordingly.

In certain circumstances, the developer may need to disclose confidential information. The agreement could set forth the circumstances, if any, when the developer can disclose confidential information without the company's prior written consent, *e.g.,* when (a) negotiating, discussing, and consulting with designated company employees; (b) purchasing

certain goods and services for the company; and (c) preparing confidential estimates, bids, or proposals. Alternatively, the developer can be required to seek the company's prior written consent for all disclosures.

6.4. REQUIRED DISCLOSURE. If Recipient or its agents or representatives are required by order of a court or other governmental entity to disclose any Confidential Information, it shall provide the Discloser with prompt prior written notice of such requirement so that the Discloser may seek a protective order or other appropriate remedy and/or waive compliance with the terms of this Agreement. If such protective order or other remedy is not obtained, or Discloser waives compliance with the provisions of this Agreement, Recipient agrees to furnish only that portion of the Confidential Information that it is legally required to furnish, in the written opinion of counsel, and to exercise best efforts to obtain assurance that the Confidential Information thus disclosed will be afforded confidential treatment.

6.5. INJUNCTIVE RELIEF. Recipient acknowledges and agrees that the disclosure of Confidential Information and the breach of the provisions of this Agreement may give rise to irreparable injury to Discloser that cannot be adequately compensated with monetary damages. Recipient further agrees that the Discloser may seek and obtain injunctive relief against the breach or threatened breach of any of the provisions of this Agreement and/or specific enforcement of such provisions in addition to any other legal or equitable remedies that may be available.

6.6. RETURN OF INFORMATION. Within 20 days after the date of termination, expiration, or cancellation of this Agreement, Recipient will promptly return to Discloser all Confidential Information in its possession or in the possession of its agents and representatives, and will promptly destroy all copies of any analyses, compilations, summaries, derivations, studies, or any other documents or tangible media that contain or reflect any Confidential Information. On request by Discloser, Recipient shall furnish Discloser with a certificate signed by an executive officer of the Recipient verifying that the same has been done.

Comment: In some cases, the company may wish to grant the developer the right to retain copies of certain documents to be used solely for the developer's internal historical and legal references.

6.7. SURVIVAL. This Section 7 shall survive the termination or expiration of this Agreement.

7. TERM AND TERMINATION OF AGREEMENT

7.1. TERM. This Agreement shall be effective from the date when it is executed and shall continue in effect until (a) terminated by Company on _ _[*number*]_ _ days prior written notice, (b) terminated under any other provision of this Agreement, or (c) until completion of all services contemplated by this Agreement (the "Term").

7.2. TERMINATION. Company may terminate this Agreement, effective immediately on written notice to Developer, if Developer should fail to do any of the following and such breach or failure continues for a period of 30 days after Developer's receipt of written notice thereof: (a) perform any material obligation under this Agreement, (b) achieve a milestone or comply with the Delivery Date under the Development Schedule set forth in Exhibit B, or (c) cure any material breach under this Agreement or any delay under the Development Schedule.

Comment: The notice period will need to be changed if the project has a fixed date by when the work product must be delivered to the company. In addition, consider imposing discounts against payments otherwise due if the developer fails to meet a milestone or the delivery date. These discounts provide a financial incentive for the developer to perform its obligations in accordance with the milestones and delivery date. Alternatively, the developer could be entitled to a bonus for on-time or early delivery.

8. INDEPENDENT CONTRACTOR STATUS. Nothing contained in this Agreement shall be construed to make either Company or Developer partners, joint venturers, principals, agents, or employees of the other. Developer shall have no express or implied authority to act for or on behalf of Company. No officer, director, employee, agent, affiliate, or contractor retained by Developer to perform work on Company's behalf under this Agreement shall be deemed to be an employee, agent, or contractor of Company. Because Company is relying on Developer's skills and experience in the performance of its services under this Agreement, Developer alone shall be responsible for determining the method, details, and means of performing such services.

9. PAYMENT OF TAXES AND BENEFITS. Developer is solely responsible for the payment of all income,

disability, withholding, and other employment taxes as well as all medical benefit premiums, vacation pay, sick pay, or other fringe benefits resulting from its retention of any officers, directors, employees, agents, affiliates, or contractors. Developer shall indemnify, defend, and hold Company, its officers, directors, agents, employees, and affiliated entities harmless from any claim for any such tax or benefit payment, including, without limitation, any penalties, fines, and interest. Developer shall maintain accurate and complete records of its compliance with the terms and conditions of this Agreement, including, without limitation, records of its payment of all taxes and benefit payments as set forth above. Personnel employed by Developer who perform duties related to this Agreement shall remain under the supervision, management, and control of Developer.

10. GOVERNING LAW. This Agreement shall be construed according to, and the rights of the parties shall be governed by, the law of the State of California without regard to its conflicts-of-laws rules. The parties hereby acknowledge and agree that any provisions of any state law adopting exactly or in modified form the Uniform Computer Information Transactions Act (UCITA) shall not apply to this Agreement. Furthermore, both parties waive any and all rights arising from any such law.

11. ATTORNEY FEES. If any legal action is necessary to enforce the terms of this Agreement, the prevailing party shall be entitled to reasonable attorney fees in addition to any other relief to which that party may be entitled.

12. ENTIRE AGREEMENT. This Agreement, together with its Exhibits, sets forth the entire agreement between the parties with regard to the subject matter hereof. No other agreements, representations, or warranties, whether oral or written, have been made by either party to the other with respect to the subject matter of this Agreement.

13. SEVERABILITY. If a court of competent jurisdiction should find any of the provisions of this Agreement to be invalid or unenforceable, those provisions shall be severable from the remainder of this Agreement and shall not cause the invalidity or unenforceability of the remainder of this Agreement.

14. AMENDMENT AND ASSIGNMENT. This Agreement may be amended only by a written agreement signed by both parties. Developer may not assign or otherwise transfer this Agreement, in whole or in part, whether voluntarily or by operation of law, including by way of sale of assets, merger, or consolidation, without the prior written consent of Company.

15. NOTICES. Any notice required or permitted under the terms of this Agreement or required by law must be in writing and must be (a) delivered in person, (b) sent by first class registered mail, or air mail, as appropriate, or (c) sent by overnight air courier, in each case properly posted and fully prepaid to the appropriate address set forth below. Either party may change its address for notice by giving notice to the other party in accordance with this Section. Notices will be considered to have been given at the time of actual delivery in person, 3 business days after deposit in the mail as set forth above, or 1 day after delivery to an overnight air courier service. The parties' notice addresses shall be as follows:

_ _[*Company's address*]_ _

_ _[*Developer's address*]_ _

IN WITNESS WHEREOF, the parties hereto have executed this Agreement, on the date(s) written below, by their duly authorized representatives.

Date: _ _ _ _ _ _

_ _[*NAME OF COMPANY*]_ _,
a _ _[*state of incorporation*]_ _ **corporation**

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

Date: _ _ _ _ _ _

_ _[*NAME OF DEVELOPER*]_ _,
a _ _[*state of incorporation*]_ _ **corporation**

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _

Its: _ _[*Title*]_ _

© The Regents of the University of California

IV. SOFTWARE EVALUATION

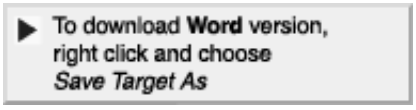
§13.4 A. Introduction

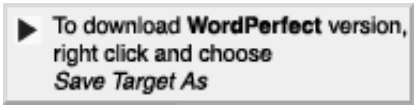
Online businesses typically experience a fast-paced software development cycle. Implementation of new improvements and features to a website provides marketing advantages and meets customer expectations for continued technological innovation. As a result, website sponsors need expedited methodologies for software development and testing. One way of expediting software development is to identify individuals or user groups to test software code in development and provide feedback and error reports. This evaluation process allows businesses to test-run their products and fix errors before the end of the development cycle in order to provide their end users with software free of bugs or other problems. It also allows the testing companies to have access to new technologies early and to help shape development of new tools and products to meet their own needs, thus gaining a potential advantage against their competitors. In §13.5 is a sample testing and evaluation agreement used to permit a third party to evaluate and comment on software in advance of the software's completion and launch.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/13 Software Development Agreements/§13.5 B. Form: Software Test and Evaluation Agreement

§13.5 B. Form: Software Test and Evaluation Agreement





SOFTWARE TEST AND EVALUATION AGREEMENT

This Software Test and Evaluation Agreement ("Agreement"), dated _ _[*date*]_ _ (the "Effective Date"), is made and entered into by and between _ _[*name of company*]_ _ ("Company") and _ _[*name of software evaluator*]_ _ ("Recipient"). This Agreement sets forth the terms and conditions applicable to Recipient's evaluation of Company's proprietary software known as _ _[*identify software*]_ _ ("Software").

1. USE OF SOFTWARE. Company grants to Recipient the limited, nonexclusive, nontransferable, revocable right to use a single object code copy of the Software, along with any related documentation or information delivered to Recipient, solely for the purpose of evaluating and testing the Software for Recipient's internal business use, subject to the terms and conditions of this Agreement. For purposes of this Agreement, the term "Software" shall include any future versions of the Software or the related documentation that Company may, in its sole discretion, decide to provide to Recipient under this Agreement. Recipient may make copies of the Software and documentation only with Company's prior written consent. All right, title, and interest in and to the Software, the documentation, all copies thereof, any and all information and data derived from Recipient's testing and evaluation of the Software, and any and all enhancements, improvements, or innovations to the Software, regardless of whether created or conceived by Recipient or its employees or agents, shall at all times remain with Company ("Company Property"). Recipient hereby assigns and agrees to assign any and all Company Property to Company and agrees to obtain the written agreement of each employee who has access to the Software to assign all Company Property to Company.

Comment: This agreement is structured as a license by the company to the tester of the company's unfinished software product. The company may replace the version initially provided with updated versions as development of the software progresses. A key concern in this agreement is the assignment to the company of any intellectual property created during this evaluation period (such as comments and suggestions on improvements to the software). Otherwise, the company may be faced with a claim for payment by the tester if the tester's suggestions are implemented in the final version.

2. RECIPIENT'S OBLIGATIONS. Recipient's obligations under this Agreement are as follows:

(a) Recipient agrees to enter into Company's standard form confidentiality agreement attached to this Agreement as Exhibit _ _ and to comply with the terms of such agreement. Recipient shall not, and shall not authorize or enable any third party to, reverse engineer, decompile, or disassemble the Software or otherwise attempt to discover any source code of the Software.

(b) Recipient shall not rent, lease, loan, resell, transfer, sublicense, or distribute the Software or documentation to any third party or authorize any third party to do so. Recipient may not modify the Software or any portion thereof.

(c) Recipient shall, at Company's request (and in any case on the expiration or earlier termination of this Agreement), promptly remove, return, or destroy the Software, including all diskettes, documentation, or other materials furnished to Recipient by Company under this Agreement (and all copies thereof).

(d) Recipient shall ensure that all data and systems used in connection with the Software are backed up at least daily and assumes all risk of loss of such data and systems due to any failure of the Software.

4. TEST COORDINATOR. Recipient shall, within 5 days of installation of the Software, designate an individual responsible for supervising Recipient's use of the Software (the "Test Coordinator"), and shall provide written notice to Company containing the name of this individual, along with all relevant contact information. The Test

Coordinator shall at all times maintain an accurate record of the authorized users of the Software and the location of the Software and all related documentation in the possession or control of Recipient and shall furnish such record to Company promptly on request.

Comment: Given the pace of development and the need for clear communication, establishing a coordinator and single points of contact for both parties will be helpful. See Section 7 for a provision identifying contact persons for each party.

5. EVALUATIONS. At least once a month during the term of this Agreement, Recipient shall provide Company with _ _[*oral/written*]_ _ evaluations of the Software, which shall include, without limitation, results and recommendations related to the use of the Software. Any oral evaluations will be either in person or by teleconference. Recipient will also provide Company with Recipient's user input and reactions to the Software's utility and business applicability. Company shall have an unrestricted, worldwide, perpetual, irrevocable, fully paid, royalty-free right and license to use and disclose, in any manner that Company considers appropriate, any information or data contained in Recipient's evaluations for any purpose whatsoever, including, without limitation, for purposes of modifying, improving, correcting, enhancing, marketing, and/or promoting the Software.

Comment: This section should specify whether there is any specific data the company would like to obtain from the tester and if so, in what format the data should be furnished to the company.

6. NO ADDITIONAL COMPENSATION. Recipient acknowledges and agrees that no monetary payment or other form of consideration will be paid to it or its employees in connection with this Agreement, other than the benefit of having access to an advance copy of the Software and access to its functionality.

7. POINTS OF CONTACT. Recipient and Company will each identify individuals who will serve as their primary points of contact for the performance of this Agreement. The initial points of contact shall be the individuals identified below and such individuals may be replaced by their respective employer on written notice to the other party.

Company Point of Contact: _ _[*name and contact information, e.g., phone number*]**_ _**

Recipient Point of Contact: _ _[*name and contact information, e.g., phone number*]**_ _**

8. NO WARRANTY. Recipient understands and acknowledges that the Software may not be in final form or fully functional, may contain errors, design flaws, or other problems, and may result in unpredictable performance, including loss of data or other damage. In view of the developmental nature of the Software, Company makes no warranties whatsoever as to the operational performance of the Software or to the compatibility between the Software and any future versions of the Software or other third party software products. Company is providing the Software to Recipient "AS IS" without warranty of any kind. COMPANY EXPRESSLY DISCLAIMS ANY AND ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT, AS WELL AS ANY WARRANTIES ALLEGED TO HAVE ARISEN FROM CUSTOM, USAGE, OR PAST DEALINGS BETWEEN THE PARTIES. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, COMPANY EXPRESSLY DISCLAIMS ANY WARRANTY, RESPONSIBILITY, OR LIABILITY FOR THE ABILITY OR FUNCTIONALITY OF RECIPIENT'S HARDWARE, SOFTWARE, FIRMWARE, OR COMPUTER SYSTEMS WITH RESPECT TO DATE-RELATED DATA, AND MAKES NO WARRANTY THAT THE SOFTWARE OR ANY OTHER SERVICES PROVIDED WILL FUNCTION WITH RECIPIENT'S SYSTEMS. This Section shall survive the expiration or earlier termination of this Agreement.

9. LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY LAW, COMPANY SHALL HAVE NO LIABILITY FOR ANY DAMAGES OF ANY KIND (INCLUDING WITHOUT LIMITATION INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR TORT DAMAGES, LOST PROFITS, OR LOST DATA) IN CONNECTION WITH THIS AGREEMENT, EVEN IF COMPANY HAS BEEN ADVISED OR IS AWARE OF THE POSSIBILITY OF SUCH DAMAGES. This Section shall survive the expiration or earlier termination of this Agreement.

Comment: Because the software is an evaluation copy of a work in process, the company should clearly limit its liability and disclaim all warranties. The tester should consider how to protect its other systems and data from any failure of the software, in order to maintain the integrity of its own systems.

10. TERM. The term of this Agreement shall commence on the Effective Date stated in the opening paragraph and shall continue in effect for _ _[*number*]_ _ months, or such longer time as the parties may agree in writing. Either party may terminate this Agreement at any time with or without cause on written notice of termination to the other party.

Comment: Testing and evaluation agreements are usually short term; *e.g.,* 3 to 6 months.

11. NO OBLIGATION. Recipient shall have no obligation to purchase software from Company. Company is under no obligation to develop or market the Software or to provide any updates or new versions of the Software to Recipient.

12. GENERAL PROVISIONS. The parties agree to the following provisions, which shall survive the expiration or earlier termination of this Agreement:

(a) Recipient may not assign its rights or delegate its duties or obligations under this Agreement without Company's prior written consent.

(b) Recipient acknowledges that a violation of this Agreement may cause irreparable harm to Company for which monetary damages would be inadequate, and agrees that, in addition to any other remedies provided by law, Company shall be entitled to seek injunctive relief against any such violation without having to post bond.

(c) If a court of competent jurisdiction holds any provision of this Agreement to be invalid or unenforceable, the remaining provisions will remain in full force and effect.

(d) The waiver by either party of any default or breach of this Agreement will not constitute a waiver of any other or subsequent default or breach.

(e) This Agreement constitutes the entire agreement between the parties with respect to its subject matter and supersedes any and all prior agreements and understandings, oral or written, and all other communications between the parties relating to its subject.

(f) This Agreement shall be governed by and construed in accordance with the laws of the State of California, U.S.A., excluding its conflict of law rules.

(g) This Agreement may be executed in one or more counterparts, each of which shall constitute an original, and all of which taken together shall constitute the same document.

Date: _ _ _ _ _ _

_ _[*NAME OF COMPANY*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _
_ _[*Company's address*]_ _

Date: _ _ _ _ _ _

_ _[*NAME OF RECIPIENT*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _
_ _[*Recipient's address*]_ _

© The Regents of the University of California

14

Content Clearances, Licensing, and Fair Use

I. INTRODUCTION §14.1

II. STEP 1: IDENTIFY THIRD PARTY ELEMENTS §14.2

III. STEP 2: DETERMINE IF THIRD PARTY ELEMENTS ARE PROTECTED BY COPYRIGHT OR OTHER INTELLECTUAL PROPERTY LAWS §14.3

IV. STEP 3: FOR PROTECTED ELEMENTS, DETERMINE WHICH OF OWNER'S EXCLUSIVE RIGHTS ARE IMPLICATED §14.4

V. STEP 4: DETERMINE IF USE IS EXEMPT FROM INFRINGEMENT LIABILITY
- A. Public Domain §14.5
- B. Fair Use §14.6

VI. STEP 5: IDENTIFY OWNERS OF WORK §14.7

VII. STEP 6: OBTAIN RIGHTS NECESSARY TO USE WORK §14.8
- A. Individual Release (Videotape of Testimonial)
  - 1. Introduction §14.9
  - 2. Form: Endorsement Agreement §14.10
- B. Still Photograph License
  - 1. Introduction §14.11
  - 2. Form: Still Photograph License §14.12
- C. Reprint Rights License
  - 1. Introduction §14.13
  - 2. Form: Digital Reprint Rights License §14.14
- D. Streaming Video License
  - 1. Introduction §14.15
  - 2. Form: Streaming Video License §14.16
- E. Special Issues in Music Licensing §14.17
- F. Creative Commons and Other Innovative Licensing Solutions §14.18

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/14 Content Clearances, Licensing, and Fair Use/§14.1 I. INTRODUCTION

§14.1 I. INTRODUCTION

Before launching, updating, or revising an Internet website, a website operator should consult with counsel to review the website content and determine whether all required licenses and rights to the content have been obtained. The following six basic steps are fundamental to the process of obtaining rights to third party content for use on a website:

- Identifying the elements of the work desired to be used.
- Determining whether those elements are or may be protected by copyright, trademark, patent, or other intellectual property laws.
- If the work is protected, identifying which of the owner's exclusive rights are implicated by the proposed use. See 17 USC §106; §1.6.
- Determining whether the proposed use may be exempt from infringement liability. (For example, an important and often misunderstood defense to copyright infringement is "fair use" as defined in 17 USC §107. See generally §§1.18-1.22.)
- Identifying the owners of the rights implicated by the proposed use.
- Obtaining the rights needed to use the work from the owners.

Sections 14.2-14.16 review these steps and provide an outline of the types of issues facing companies with an online presence in obtaining rights to use third party intellectual property, along with possible contractual or other solutions to those issues. Although §§14.2-14.16 focus primarily on the licensing of copyrighted works, trademark and patent issues may need to be addressed as well.

NOTE: Counsel preparing software license agreements and other software contracts for use in an online environment should be familiar with the electronic contracting issues discussed in chap 7.

© The Regents of the University of California

§14.2 II. STEP 1: IDENTIFY THIRD PARTY ELEMENTS

The website and its elements should be reviewed with the following questions in mind:

- What is the source of the clip art, photographs, and other graphical elements appearing on the site? Is this material either owned by the website sponsor or properly licensed from third parties? (See, *e.g.,* the still photograph license in §§14.11-14.12.)
- Is there any music or video streamed or downloadable from the site? (See, *e.g.,* the streaming video license in §§14.15-14.16.) Are software programs downloadable from the site? Have all applicable licenses for such streaming or downloading been obtained?
- Are any names, photographs, likenesses, or voices of, or testimonials from, individuals used on the site? Have those individuals consented to the use of their names, images, words, or voices? (See the individual release agreement in §§14.9-14.10.)
- Does the site contain text or excerpts of text written by third parties? Research, scholarly material, news articles, poems, and lyrics are all protected by copyright and, unless a fair use exemption applies, a license from the author will be required.
- Are there any third party trademarks used on the site or in the metatags associated with the site? If so, have the trademark owners provided their consent? Is it clear that use of the third party trademarks is not intended to appear as an endorsement of the products or services offered? (See §3.56 for a sample trademark license and §§3.71-3.76 for a discussion of the use of trademarks as metatag data.)
- Does the site contain any links to third party sites? Check the user and linking policies of those sites to determine if the link is compliant. (See §8.18 for a sample linking agreement.)
- Was all the software used to operate the site developed by the company or its employees? If the software was obtained from a third party such as a software developer or downloaded from the Internet, have license rights (or an assignment of rights) been obtained? Is the proposed use in compliance with the license agreement? (See §7.3 for a discussion, and §8.5 for a form, of click-wrap license agreement, and §§8.4-8.13 for a discussion and forms of online software licenses. See also chap 12 on software license agreements, and §§5.4-5.25 on website development agreements. All of these types of agreements may control ownership and other rights in the content and technology of a website.)

© The Regents of the University of California

§14.3 III. STEP 2: DETERMINE IF THIRD PARTY ELEMENTS ARE PROTECTED BY COPYRIGHT OR OTHER INTELLECTUAL PROPERTY LAWS

Any element of a company's website that was not generated internally by the company or its employees should be reviewed for copyright issues. A work is protected by copyright law if it is an "original work of authorship fixed in a tangible medium of expression." 17 USC §102(a). Graphics images, music, software programs, photos, text, and similar elements of a website may be protected by copyright, regardless of format. While copyright protects the tangible expression of an idea, the idea itself is not protected. 17 USC §102(b). See §§1.1-1.23 for a more detailed discussion of copyright law. Concepts, ideas, business methods, processes, and inventions may be protectible under patent or trade secret law. Software and website business models should be analyzed with these issues in mind. See chap 2 for a more detailed discussion of patent and trade secret laws.

© The Regents of the University of California

§14.4 IV. STEP 3: FOR PROTECTED ELEMENTS, DETERMINE WHICH OF OWNER'S EXCLUSIVE RIGHTS ARE IMPLICATED

The exclusive rights of a copyright owner are outlined in §1.6. Examples of rights that may be implicated in website development are:

- The right to reproduce the work. 17 USC §106(1). To permit graphics, music, or other copyrightable elements to be downloaded to end users, the website operator must have obtained the right to make and distribute copies. In addition, the activities involved in creating and maintaining the site usually require that copies of the work be made.
- The right to prepare derivative works. 17 USC §106(2). If graphical or photographic elements are combined with music and text in a multimedia show or animated sequence on the site, the act of creating those combined works would infringe this right without a license from the owner.
- The right to distribute copies of the work to the public. 17 USC §106(3). Providing music or video for downloading without a license from the copyright owner would infringe the owner's distribution rights.
- The right to perform the work publicly. 17 USC §106(4). Streaming audio (either music or spoken words) without a license from the copyright owner would infringe the owner's performance rights.
- The right to publicly display works. 17 USC §106(5). All visible or audible elements of a website could potentially infringe this right.

The rights of a patent holder as the holder of a federally authorized monopoly are the rights to manufacture, use, license, offer for sale, sell, and import the subject matter of the patent, and to exclude others from doing so. For a general discussion of patent law, see §§2.1-2.19. If any software functionality proposed to be used on a website is covered by a patent (see §2.19), unlicensed use of that software would infringe the patent holder's rights.

Two kinds of trade secret rights may be implicated in connection with the preparation of a website: (1) trade secret rights of the company preparing to launch the website, and (2) trade secret rights of third parties that may be disclosed on the website. Because trade secret protection is normally lost once a trade secret becomes generally known (see §2.24), it is critical that a new website not be released online until the company is certain that the website does not reveal any confidential trade secret information, either on the face of the website or in hidden data or code. Because a trade secret derives its value from its confidentiality, the entire website must be reviewed for content—such as customer information, financial information, future business plans, or unprotected access to website software source code—potentially subject to a loss of trade secret protection.

© The Regents of the University of California

V. STEP 4: DETERMINE IF USE IS EXEMPT FROM INFRINGEMENT LIABILITY

§14.5 A. Public Domain

A work in the public domain is a work whose copyright has expired, or that has been dedicated to the public domain by its creator. See, *e.g.,* http://creativecommons.org/licenses/publicdomain. Use of works in the public domain will not subject the user to liability for copyright infringement. Works in the public domain include those published before 1923 and those published before 1978 without a copyright notice. See generally §1.3. Works created by the United States government are not subject to copyright protection, but works created by independent contractors of the U.S. government may be copyrighted. See 17 USC §105. See, *e.g.,* Federal Acquisition Regulations (48 CFR §§12.212, 52.227-14). Ideas, concepts, and facts cannot be copyrighted (see §1.2), but patent or trade secret protection may apply (see chap 2).

PRACTICE TIP: When in doubt, counsel should assume that every element of a website not actually created by company employees for the occasion is protected by intellectual property rights held by a third party. Merely because software, graphical elements, music, or research materials can be downloaded from the Internet does not mean that those elements are in the public domain or that they are free for unrestricted use. As noted above, for a work to be in the public domain, the copyright must have expired, or else the copyright owner must have expressly granted the copyright to the public domain.

© The Regents of the University of California

§14.6 B. Fair Use

Fair use of a copyrighted work will not subject the user to infringement liability. Section 107 of the Copyright Act (17 USC §107) provides that "fair use" of a work for purposes such as "criticism, comment, news reporting, teaching… scholarship or research" does not constitute copyright infringement. See §§1.18-1.22 for a general discussion of the doctrine of fair use. The Copyright Act does not define "fair use." Instead, it sets out four nonexclusive factors to be considered in determining whether or not a particular use is "fair." See §1.18. Application of the doctrine of fair use has been the subject of much litigation, and courts have a significant amount of discretion in deciding fair use cases. There is no "bright line" for determining what is or is not fair use of a copyrighted work, and each determination depends on the specific facts of the use of the work. See §§1.18-1.22.

© The Regents of the University of California

§14.7 VI. STEP 5: IDENTIFY OWNERS OF WORK

Locating the owners of the intellectual property desired to be used in development and operation of a website may be quite challenging. For copyrighted works, the following sources may be useful:

- The text of any copyright notice should include the copyright owner's name. If available, the copyright notice should be the best starting place for identifying the owner.
- The website of the United States Copyright Office has an electronic search capacity for its registration records (http://www.copyright.gov/records).
- Agencies such as Thomson & Thomson will perform searches of copyright records and provide search reports as a paid service (http://www.thomson-thomson.com).
- Licensing agencies, such as the following, maintain records of copyright owners:
- Text: Copyright Clearance Center (http://www.copyright.com).
- Music: ASCAP (http://www.ascap.com) or BMI (http://www.bmi.com) for public performance rights; the Harry Fox Agency (http://www.harryfox.com) for mechanical rights.
- Motion Pictures: Motion Picture Licensing Corporation (http://www.mplc.com).
- Plays: Samuel French, Inc., 45 West 25th Street, NY, NY 10010-2751 (http://www.samuelfrench.com).
- Photography: American Society of Media Photographers (http://www.asmp.org).

PRACTICE TIP: If, after searching, a company is unable to identify and locate the copyright owner in order to obtain permission, the work should not be used.

© The Regents of the University of California

§14.8 VII. STEP 6: OBTAIN RIGHTS NECESSARY TO USE WORK

A website operator will need to obtain licenses from the owners of the intellectual property that the operator wishes to use in the development and operation of its site. In §§14.9-14.15 are sample license agreements for different types of copyrighted content frequently used in websites.

PRACTICE TIP: Counsel should read the license terms for downloadable works carefully. For example, if the online license permits "personal noncommercial use only," use of the work for a commercial website is effectively precluded. This restriction is common in online licenses for free downloads.

See chap 7 for a discussion of electronic acceptance of contracts and "click-wrap" agreements.

© The Regents of the University of California

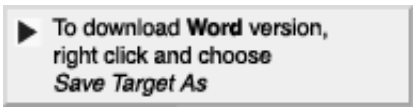
A. Individual Release (Videotape of Testimonial)

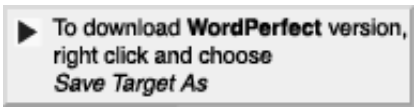
§14.9 1. Introduction

Many websites established for e-commerce or marketing purposes contain user or customer reviews of the sponsoring company's products or services. Such reviews may be text-based, possibly accompanied by a photograph of the individual user, or in video format. The endorsement agreement in §14.10 is intended to be used to obtain appropriate license rights along with the review itself. Note that the terms of this model form are quite broad, and could be narrowed if desired by the user.

© The Regents of the University of California

§14.10 2. Form: Endorsement Agreement





ENDORSEMENT AGREEMENT

For good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, I, the undersigned, agree as follows:

1. I agree to be photographed, recorded, and videotaped by _ _[*name of website operator*]_ _ and its agents ("Company").

2. I hereby irrevocably authorize Company and its affiliates to copyright, publish, reproduce, exhibit, transmit, broadcast, televise, digitize, display, otherwise use, and permit others to use, (a) my name, image, likeness, and voice, and (b) all photographs, recordings, videotapes, audiovisual materials, writings, statements, and quotations of or by myself and furnished to the Company by me (collectively, the "Materials"), in any manner, form, or format whatsoever now or hereinafter created, including on the Internet, and for any purpose, including, but not limited to, advertising or promotion of Company, its affiliates, or their services, without further consent from or payment to me.

3. It is understood that all of the Materials, and all films, audiotapes, videotapes, reproductions, media, plates, negatives, photocopies, and electronic and digital copies of the Materials, are the sole property of Company. I agree not to contest the rights or authority granted to Company hereunder. I hereby forever release and discharge Company, its employees, licensees, agents, successors, and assigns from any claims, actions, damages, liabilities, costs, or demands whatsoever arising by reason of defamation, invasion of privacy, right of publicity, copyright infringement, or any other personal or property rights from or related to any use of the Materials. I understand that Company is under no obligation to use the Materials.

4. This document contains the entire agreement between the Company and the undersigned concerning the subject matter hereof. This agreement shall be governed by and construed in accordance with the laws of the State of California without regard to conflicts of law rules. I agree to execute any further documents or instruments requested by Company in order to evidence or confirm these rights.

Date: _ _ _ _ _ _ __[*Signature*]__
_ _[*Typed name*]_ _

_ _[*Address*]_ _
_ _[*City, State, Zip*]_ _

© The Regents of the University of California

B. Still Photograph License

§14.11 1. Introduction

The still photograph license agreement in §14.12 is intended to grant the right to use a still photograph obtained from the copyright owner off the Internet. Note that the limitation of liability language in Section 3 of the form is one-sided in favor of the licensor. If the licensee has leverage in the transaction, the licensee should seek to eliminate or increase the cap on liability, because the price paid for the image may bear no relationship to the injured party's damages for unauthorized use of his or her photograph or graphics image.

© The Regents of the University of California

§14.12 2. Form: Still Photograph License

▶ To download **Word** version, right click and choose *Save Target As*

▶ To download **WordPerfect** version, right click and choose *Save Target As*

STILL PHOTOGRAPH LICENSE

The terms and conditions of your license for the use of one or more _ _[*name of owner of images*]_ _ ("Company") images are set forth below. Please read this license agreement carefully. By placing an order for a Company image, you are agreeing to be bound by the terms and conditions of this Still Photograph License (this "Agreement") with respect to each Company image that you select.

1. LICENSE. Company grants you the nonexclusive right to use the image you have selected from our website for any single use within the Use Category that you indicate below. If you order more than one image, each image may be used only for the Use Category that you indicate when you order the image. You are not permitted to use the image, or any portion of the image, in any other way. Furthermore, you may not use the image in any manner that is defamatory or pornographic or otherwise violates any applicable laws. The Company reserves all rights except those specifically granted in this Agreement. This Agreement is effective as of the date and time that you electronically accept this Agreement.

2. PAYMENT. You agree to pay Company the Image License Fees set forth in the Image Catalog below for each image, with payment due and payable before your downloading of the image. The license granted to you under this Agreement becomes effective only on receipt by Company of your payment in full.

3. WARRANTY; LIABILITY. Company warrants to you that it has the right to grant this license to you, and that all necessary model and other releases have been obtained. Your sole and exclusive remedy for a breach of these warranties is a refund of the price you pay to Company to license the image. Company makes no other warranty, express or implied, including, without limitation, any implied warranties of merchantability or fitness for a particular purpose. In no event shall Company or any of its affiliates be liable for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of the use of or inability to use any image licensed hereunder. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

4. ASSIGNMENT. *Copies; Notice of Copyright.* You may not transfer or assign this license to a third party. You may not make copies, either digital or printed, of the image for the purpose of relicensing or reselling the image (whether separately or in combination with other images) or for any other purpose except those expressly set forth in the Use Category you select for the image. Likewise, you may not copy the image file for the purpose of transferring it, whether by gift or sale, to anyone else unless such use of the image is expressly included within the Use Category you select for such image. You shall ensure that the copyright notices contained in the downloaded file of each image are not removed or altered and are prominently displayed to viewers of the Company's images.

5. GENERAL. This Agreement constitutes the entire agreement between you and Company concerning the license of the image or images you select. This Agreement is governed by the laws of the State of California and the United States. All rights to Company images are owned by Company and its licensors and are protected by United States copyright laws, international treaty provisions, and other applicable laws. Company retains all rights not expressly granted by this Agreement. The license granted by this Agreement shall terminate immediately and automatically without notice from Company if you fail to comply with any of the terms or conditions of this license agreement.

IMAGE ORDER FORM

A. Using the form below, please identify the image file number(s) of the image(s) you wish to acquire next to the Use Category for which you wish to license each image. The applicable fee appears in the catalog next to

the image. If you wish to license more than one image in a particular Use Category, please duplicate this form and total the last page. Please provide your name on each form, but your address and credit card information is only needed on the last page.

IMAGE FILE #	USE CATEGORY	$ FEE
_____	Personal noncommercial use	_____
_____	Personal noncommercial website use	_____
_____	Commercial internet use	_____
_____	Commercial use (other than on the Internet)	_____
_____	Commercial display (other than on the Internet)	_____
	TOTAL	_____

B. Indicate the delivery method you prefer:

_____ An attached JPEG file sent to your e-mail address.

_____ A download from our Web page. (If you choose this method, you will be notified by e-mail of the Web address when the image file is ready for downloading and will be sent a key to permit you to access the image file on line).

C. Your name (end user of license), address, and credit card data:

Your Name & Company:

_____

_____

Address: _____

_____

City: _____ State: _____ Zip: _____

Country: _____

Phone Number: _____ Fax: _____

E-mail Address: _____

Type of credit card*: _____

Name on card: _____

Credit card account #: _____

Expiration date: _____

In most cases, your order will be processed immediately and the digital image(s) will be uploaded for delivery within a few hours.

***We accept VISA, MasterCard, American Express, or Discover Card**

© The Regents of the University of California

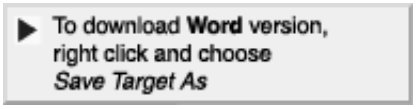
C. Reprint Rights License

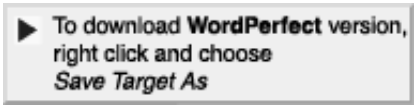
§14.13 1. Introduction

The reprint rights license agreement in §14.14 is intended for use in connection with the electronic reproduction of text such as an article or the display of an electronic book (eBook) on a web site. It can be adapted for use with other textual content.

© The Regents of the University of California

§14.14 2. Form: Digital Reprint Rights License





DIGITAL REPRINT RIGHTS LICENSE AGREEMENT

You agree that this Digital Reprint Rights License Agreement (this "Agreement") is a binding contract between _ _[*website operator*]_ _ and its successors and assigns (collectively, the "Company") and you.

California law shall apply to this Agreement, without regard to its conflict of law principles.

Subject to the terms and conditions of this Agreement, the Company hereby grants you a nonexclusive, nontransferable, limited license (the "License") to the digital reprint rights for _ _[*name of book*]_ _ (the "eBook") in any digital format from which the content of the eBook may be read.

The term "digital reprint rights" means that you may sublicense digital copies of the eBook by electronic distribution based on your possession of a digital copy of the eBook, which are available on the Company's download page.

This License does not include the right to repackage and sell the eBook or recordings thereof in physical or hardcopy form (for example, in print or on CD-ROM or cassette). You may only sublicense directly to end users and not to resellers or distributors.

You agree to the following terms and conditions:

1. THE DIGITAL REPRINT RIGHTS DESCRIBED IN THIS AGREEMENT ARE BEING PURCHASED FOR THE LICENSE FEES LISTED BELOW. THE COMPANY MAKES NO WARRANTY OR GUARANTEE OF ANY KIND (INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT) WITH REGARD TO THE EBOOK, WHICH IS PROVIDED "AS IS".

2. In all sales of digital reprints, you shall include the copyright notices for the eBook provided in this download.

3. You shall not make any modifications or alternations to the eBook; you may offer the products only in their original edition. You shall not record the eBook or any portion thereof or translate the eBook into other languages or formats.

4. You may sublicense the eBook thereof at any retail price or give digital reprints of the eBook away as an incentive or bonus.

5. You acknowledge and agree that you do not have any right, license, or title to the master reprint rights of the eBook, meaning that you shall not sell reprint rights for the eBook.

6. You acknowledge and agree that this License does not include any support services.

By placing an order for this product, you acknowledge that you have read and accepted the terms of this Agreement. You will be e-mailed access to the download page to download your copy of the eBook transcripts as soon as they are produced. Please download these to your server. If you choose to market these products to end users, downloading to end users shall take place from your server.

© The Regents of the University of California

D. Streaming Video License

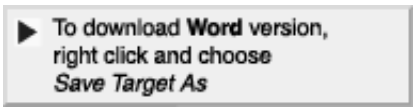
§14.15 1. Introduction

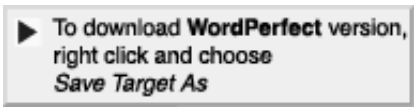
The streaming video license agreement in §14.16 is used in connection with streaming video and can also be adapted for use with streaming audio. The parties should consider whether the payment arrangements in Section 7 of the form should be structured as a flat fee (as here), a payment based on the number of viewings of the content, or a royalty payment based on a percentage of the revenue that the licensee receives from end users with respect to the content.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/14 Content Clearances, Licensing, and Fair Use/§14.16 2. Form: Streaming Video License

§14.16 2. Form: Streaming Video License





STREAMING VIDEO LICENSE

Please read this Streaming Video License (this "Agreement") carefully before proceeding to download video. This Agreement licenses video content to you from _ _[*company name*]_ _ (the "Company") and contains warranty and liability disclaimers. By selecting the Order button on the product page, you are confirming that you have read and understand this Agreement, and agree to be bound by the terms of this Agreement. If you do not agree with the terms of this Agreement, do not select the Order button on the product page.

1. DEFINITIONS.

(a) "*Company Content*" means the digital video content known as _ _[*specify*]_ _.

(b) "*Key*" means a code supplied to you via e-mail after purchasing the Company Content to permit you to access and download the Company Content to your Internet server.

(c) "*Internet Server*" means the server(s) on which you host your Internet Site. Please insert the total number of Internet Servers: _ _[*number*]_ _.

(d) "*Internet Site*" means the following website owned and operated by you: _ _[*website address*]_ _.

(e) "*License*" means the electronic permission granted to you under this Agreement for the purpose of playing the Company Content on your Internet Server.

2. LIMITED LICENSE. This Agreement allows you, subject to the restrictions described below, to (a) host the Company Content on your Internet Server for display via streaming video on your Internet Site using _ _[*name of streaming video format*]_ _ for viewing by your end users who have accepted terms of use that are at least as restrictive as this Agreement, and (b) make copies of the Company Content for back-up and archival purposes only. All rights not expressly granted are reserved. With the Key, you will be provided a single License needed for each Internet Server upon which you desire to host or run the Company Content. Once installed on your computer, a License will be in effect for the life of the copyright in Company Content.

3. RESTRICTIONS. (a) You may not make or distribute copies of the Company Content, or electronically transfer the Company Content from one computer to another or over a network. You may not decompile, reverse engineer, disassemble, or otherwise reduce the Company Content to a human-perceivable form. You may not modify, transfer, or create derivative works based on the Company Content or any part thereof. You may not export or re-export, directly or indirectly, the Company Content into any country prohibited by the United States Export Administration Act and the regulations thereunder.

(b) You understand and agree that the Company Content may transmit certain information to Company electronically and automatically. Any information received by Company from this transmission shall be used by Company solely for the purposes of diagnosing or correcting errors, improving the Company Content, or notifying you of updates regarding the Company Content. You shall secure the approval of your end users to this transmission.

(c) You may not use the Company Content to: (1) create derivative works; (2) infringe on or violate the intellectual property, privacy, publicity, or other rights of third parties, including, without limitation, the rights of any third parties in any sound recordings, musical compositions, photographs, artwork, literary creations, or other copyrightable works of any kind or nature; or (3) engage in any defamatory or slanderous conduct. All use of the Company Content shall be on the Internet Site only and not for any other purpose. The Company Content must be made available in its original form, unedited and unmodified. You agree not to superimpose

any images or text on the Company Content as it is displayed to end users and not to impair the readability of any credits or other title screens in the Company Content.

(d) You hereby agree to defend, indemnify, and hold harmless Company and its parents, subsidiaries, affiliates, successors, licensees, agents, attorneys, heirs, and assigns, and the officers, directors, and employees of the foregoing, from and against any and all third party claims, liabilities, demands, costs, and expenses (including attorney and accountant fees reasonably incurred) in connection with (1) any breach or alleged breach by you of any covenant, representation, or other provision of this Agreement, or any of your obligations hereunder; (2) your use and operation of the Internet Servers and Internet Sites; (3) any third party claims brought by your end users; and (4) the acts or omissions of your end users.

4. OWNERSHIP. The License gives you limited rights to use the Company Content. Although you obtain limited rights to use the Company Content as specified in this Agreement, you do not thereby become the owner of, and Company and its suppliers retain title to, the Company Content and all copies thereof. All rights not specifically granted in this Agreement, including federal and international copyrights, are reserved by Company and its suppliers. You agree to maintain all copyright notices appearing on the Company Content and you will not remove or alter such notices or add your copyright notice to Company Content.

5. DISCLAIMER OF WARRANTIES AND OF TECHNICAL SUPPORT.

THE COMPANY CONTENT IS PROVIDED TO YOU ON AN "AS IS" BASIS, WITHOUT ANY TECHNICAL SUPPORT OR WARRANTY OF ANY KIND FROM COMPANY, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER LEGAL RIGHTS, WHICH VARY FROM STATE TO STATE. Your sole and exclusive remedy in the event that the Company Content fails to function, or in the event of any other breach of this Agreement by Company, is to terminate this Agreement and cease all use of the Company Content.

6. LIMITATION OF DAMAGES.

(a) NEITHER COMPANY NOR ITS AFFILIATES OR SUPPLIERS SHALL BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OR LOSS (INCLUDING DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, OR THE LIKE), WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, EVEN IF COMPANY OR ITS REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL COMPANY BE LIABLE FOR AMOUNTS IN EXCESS OF WHAT YOU HAVE PAID FOR THE COMPANY CONTENT. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

(b) COMPANY'S LIABILITY TO YOU FOR ANY REASON, WHETHER BASED ON BREACH OF CONTRACT OR TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, SHALL BE LIMITED TO THE AMOUNT OF FEES YOU PAID TO COMPANY. The warranty disclaimer, exclusive remedies, and limitation of liability set forth in this Agreement are fundamental elements of the basis of the bargain between Company and you. You agree that Company would not be able to provide the Company Content on an economic basis without such limitations.

7. PAYMENT. Payment in full is due prior to download of the Company Content. Please see the product catalog for pricing information. You are responsible for payment of all taxes with respect to your use and operation of the Company Content.

**8. GENERAL. This Agreement shall be governed by the laws of the State of California without regard to its conflict of law provisions. Any disputes arising under or related in any way to this Agreement shall be heard exclusively in _ _[*name of judicial district*]_ _, California. The parties hereby consent to jurisdiction in any state or federal court located in_ _[*name of judicial district*]_ _, California and waive any claim or defense that such forum is not convenient or proper. This Agreement contains the complete agreement between the parties with respect to the subject matter hereof, and supersedes all prior or contemporaneous agreements or understandings, whether oral or written. If any part of this Agreement is held invalid or unenforceable by a court of competent jurisdiction, the remainder of the Agreement shall be interpreted so as to reasonably effect the intention of the parties. All questions concerning this Agreement shall be directed to: _ _[*name of Company*

contact]_ _.

© The Regents of the University of California

§14.17 E. Special Issues in Music Licensing

Internet businesses should be aware that the various bundles of rights in music are more complex than in other types of copyrighted works. For example, separate copyrights may be held in the underlying composition (the original sheet music), the lyrics, the arrangement of the work (for example, an orchestral arrangement of a work that was originally composed for solo guitar), and the performance or recording of the work. 17 USC §§106, 114. The right to "synchronize" music to video is also a separate copyright. Because these rights may be held by different copyright owners, separate licenses may be required. Care should be taken to make sure that all necessary rights have been obtained and that any license is broad enough to cover the anticipated uses of a work.

In the usual copyright infringement analysis, de minimis copying is not actionable. *Fisher v Dees* (9th Cir 1986) 794 F2d 432. In the case of music, the analysis of whether a de minimis exception applies is more complex. The Sixth Circuit recently held that all "samplings" of sound recordings, no matter how small, are infringing. *Bridgeport Music, Inc. v Dimension Films, Inc.* (6th Cir 2004) 383 F3d 390, 398 (substantial similarity test and de minimis analysis do not apply to digital sampling of recorded music; instead, use of music recorded by another party, no matter how small, should be licensed).

Note that the *Bridgeport* ruling applies to samplings of sound recordings (*i.e.,* recordings of music performances). The Ninth Circuit has ruled that sampling of musical compositions (*i.e.,* sheet music) is subject to the de minimis copying defense. *Newton v Diamond* (9th Cir 2003) 349 F3d 591. In *Newton,* the three-note, six-second sample made by defendants, the Beastie Boys, comprised 2 percent of the approximately five-minute song, "Choir." The Beastie Boys "looped" this sample as a background element of its work "Pass the Mic," so that the sample was heard repeatedly throughout. The court ruled that the sample was a "de minimis" or trivial instance of copying and thus not a violation. 349 F3d at 594. Note that the court implies that had the Beastie Boys sampled some more distinctive pattern of notes or had they taken more of the notes, they would have violated Newton's copyright in the composition.

© The Regents of the University of California

§14.18 F. Creative Commons and Other Innovative Licensing Solutions

Today, many works are made available online subject to permissive licenses that allow reproduction, distribution, and other uses without compensation.

The nonprofit organization Creative Commons (http://www.creativecommons.org) has created free licenses and other legal tools that allow creators to "mark creative work with the freedom the creator wants it to carry, so others can share, remix, use commercially, or any combination thereof." Creative Commons estimates that as of 2008, more than 130 million works had been licensed.

In *Jacobsen v Katzer* (Fed Cir 2008) 535 F3d 1373, 1381, the Federal Circuit held that open source licenses are enforceable, stating that "copyright holders who engage in open source licensing have the right to control the modification and distribution of copyrighted material."

Similarly, Wikipedia (http://www.wikipedia.org) and other content is licensed under the GNU Free Documentation License, which is "intended for use on a manual, textbook or other document to assure everyone the effective freedom to copy and redistribute it, with or without modifications, either commercially or non-commercially." See http://www.gnu.org/licenses/licenses.html.

© The Regents of the University of California

15

Source Code Escrows

I. INTRODUCTION §15.1

II. FORM: SOURCE CODE ESCROW AGREEMENT §15.2

© The Regents of the University of California

§15.1 I. INTRODUCTION

An online business depends on the stability of the software that runs its website and its ability to update and adapt the software code to the changing technological landscape of the market and upgrades in end-user systems. An Internet business that licenses its core software from a third party may be dependent on that third party for continued support and access to essential upgrades and customizations.

Software code provided by a third party licensor is often furnished in "object code" form only. Object code is that version of the software program in machine language, *i.e.,* a series of binary numbers that a computer processor can understand but that is essentially impossible for a person to read or modify. The original work product of a software programmer is a series of commands written in programming language (such as hypertext markup language (html)) and known as "source code." Source code is normally readable by persons familiar with the programming language used. Object code is created from source code by a program known as a compiler. In order to modify, upgrade, or customize the software, access to the source code is required. Many vendors restrict access to their source code to preserve for themselves the revenue to be derived from ongoing upgrade work and, importantly, to protect and preserve the trade secrets embodied in the source code.

If the software vendor defaults on its maintenance and support contract, goes bankrupt, or stops supporting the code licensed by the Internet business, the business may have no way to maintain the code that forms the backbone of its online business.

Establishing a source code escrow may help address these risks. A source code escrow is a three-party agreement by which the licensor submits its source code to an escrow agent to be held and safeguarded. On the happening of some triggering event, such as a breach of the software maintenance agreement that is not cured within the time period specified in the maintenance agreement or a cessation of support of the software program by the vendor, the escrow agent releases the source code to the licensee. The licensee, on its own or through a third party, then can undertake its own maintenance and support activities.

Source code escrow services are provided by a range of enterprises. For software products that are especially valuable, use of a full-service escrow agent is desirable. Full-service escrow agents will have procedures in place to manage intellectual property assets, including provision of deposit update reminders, notification of updates, account activity summaries, and in-house technical verification of deposited materials. In addition, the escrow agent should maintain a secure, environmentally controlled vault for electronic media storage. In the present era of financial instability in the software industry, an escrow should be considered for all software that is "mission critical."

Instead of an escrow, a licensee can attempt to negotiate an up-front source code license. A source code license is likely to be more expensive, however, and the licensor may be reluctant to grant one because of confidentiality concerns. Moreover, to avoid the risk of trade secret infringement, the licensee may not wish to be "tainted" by access to the trade secrets contained in the source code. Such access may give the licensor a basis for an infringement claim if the licensee develops similar software in the future.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/15 Source Code Escrows/§15.2 II. FORM: SOURCE CODE ESCROW AGREEMENT

§15.2 II. FORM: SOURCE CODE ESCROW AGREEMENT

▶ To download **Word** version, right click and choose *Save Target As*

▶ To download **WordPerfect** version, right click and choose *Save Target As*

SOURCE CODE ESCROW AGREEMENT

This Source Code Escrow Agreement (this "Agreement"), dated to be effective _ _[*date*]_ _, is made among _ _[*name of escrow agent*]_ _ ("Escrow Agent"), _ _[*name of licensor*]_ _ ("Depositor"), and _ _[*name of licensee*]_ _ ("Licensee"), with reference to the following facts:

A. Depositor and Licensee have entered into that certain Software License Agreement dated _ _[*date*]_ _ (the "License Agreement").

B. The availability of the Source Code (as defined in the License Agreement) of Depositor is critical to Licensee in the conduct of its business contemplated by the License Agreement, and, therefore, Licensee needs access to the Source Code under certain circumstances.

C. Depositor and Licensee desire to establish an escrow with Escrow Agent to provide for the retention, administration, and controlled access of the Source Code and related materials of Depositor.

D. The parties desire this Agreement to be supplementary to the License Agreement for purposes of 11 USC §365(n).

NOW, THEREFORE, in consideration of the mutual terms and conditions set forth herein, and for good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereby agree as follows:

ARTICLE 1: DEPOSITS

1.1. *Obligation to Make Deposit.* On the execution and delivery of this Agreement by the parties, Depositor shall deliver to Escrow Agent the Source Code and related materials ("Deposit Materials") required to be deposited by the License Agreement, which materials are identified on Exhibit A attached hereto. Escrow Agent shall have no obligation with respect to the preparation, signing, or delivery of Exhibit A.

Comment: As part of the deposit, consider adding the names of employees of the depositor who will be responsible for technical maintenance of the deposited materials. In the event that those individuals leave the company, the licensee will be able to reach them if necessary to answer questions about the deposited materials.

1.2. *Identification of Tangible Media*. Prior to the delivery of the Deposit Materials to Escrow Agent, Depositor shall conspicuously label for identification each document, magnetic tape, disk, or other tangible medium upon which the Deposit Materials are written or stored. Additionally, Depositor shall complete Exhibit B to this Agreement by listing each such tangible medium by the item description, the type of medium, and the quantity. Exhibit B shall be signed by Depositor and delivered to Escrow Agent with the Deposit Materials. Unless and until Depositor makes the initial deposit with Escrow Agent, Escrow Agent shall have no obligations under this Agreement, except the obligation to notify the parties regarding the status of the deposit account as required in Section 2.2 below.

1.3. *Deposit Inspection*. When Escrow Agent receives the Deposit Materials and Exhibit B, Escrow Agent shall conduct a deposit inspection by visually matching the labeling of the tangible media containing the Deposit Materials to the item descriptions and quantity listed on Exhibit B. In addition to the deposit inspection, Licensee may elect to cause a verification of the Deposit Materials in accordance with Section 1.6 below.

1.4. *Acceptance of Deposit*. At completion of the deposit inspection, if Escrow Agent determines that the

labeling of the tangible media matches the item descriptions and quantity on Exhibit B, Escrow Agent shall date and sign Exhibit B and mail a copy thereof to Depositor and Licensee. If Escrow Agent determines that the labeling does not match the item descriptions or quantity on Exhibit B, Escrow Agent shall (a) note the discrepancies in writing on the Exhibit B; (b) date and sign Exhibit B with the exceptions noted; and (c) mail a copy of Exhibit B to Depositor and Licensee. Escrow Agent's acceptance of the deposit occurs upon the signing of Exhibit B by Escrow Agent. Delivery of the signed Exhibit B to Licensee is Licensee's notice that the Deposit Materials have been received and accepted by Escrow Agent.

1.5. *Depositor's Representations*. Depositor represents as follows:

(a) Depositor lawfully possesses all of the Deposit Materials deposited with Escrow Agent;

(b) With respect to all of the Deposit Materials, Depositor has the right and authority to grant to Escrow Agent and Licensee the rights provided in this Agreement;

(c) The Deposit Materials are not subject to any lien or other encumbrance;

(d) The Deposit Materials consist of the technological and other materials identified either in the License Agreement or Exhibit A, as the case may be; and

(e) The Deposit Materials are readable and usable in their current form or, if any portion of the Deposit Materials is encrypted, the decryption tools and decryption keys have also been deposited with the Escrow Agent as part of the Deposit Materials.

1.6. *Verification.* Licensee shall have the right, at Licensee's expense, to cause a verification of any Deposit Materials for purpose of determining the accuracy, completeness, sufficiency, and quality of the Deposit Materials. Licensee shall notify Depositor and Escrow Agent of Licensee's request for verification. Depositor shall have the right to be present at the verification. For any verification elected hereunder, only Escrow Agent, or at Escrow Agent's election an independent person or company selected and supervised by Escrow Agent, may perform the verification.

Comment: Verification of the materials deposited is necessary to ensure that the escrow agent has the correct version of the materials. Although this provision allows the escrow agent to elect an independent person to perform the verification, the depositor and the licensee can also mutually agree on a person who will perform the verification. In addition, the type of verification that needs to be performed must be determined. Is technical verification (*i.e.,* confirmation that the deposited materials operate properly) needed, or merely a verification of the contents of the deposited materials (*i.e.,* confirmation that they contain everything that the depositor is obligated to deposit)?

1.7. *Deposit Updates*. Depositor shall update the Deposit Materials within 60 days of each release of a new version of the Source Code, and add the updates to the existing deposit under this Agreement. All deposited updates shall be listed on a new Exhibit B and the new Exhibit B shall be signed by Depositor. Each Exhibit B shall be held and maintained separately within the escrow account. Escrow Agent shall create and maintain an independent record to document all updates, additions, releases, or other activity for each Exhibit B. The processing of all deposited updates shall be in accordance with Sections 1.2 through 1.6 above. All references in this Agreement to the Deposit Materials shall include the initial Deposit Materials and any updates to the Deposit Materials.

1.8. *Removal of Deposit Materials*. The Deposit Materials may be removed or exchanged only on written instructions signed by Depositor and Licensee or as otherwise provided in this Agreement.

ARTICLE 2: CONFIDENTIALITY AND RECORD KEEPING

2.1. *Confidentiality*. Escrow Agent shall maintain the Deposit Materials in a secure, environmentally safe, locked facility that is accessible only to authorized representatives of Escrow Agent. Escrow Agent shall reasonably protect the confidentiality of the Deposit Materials. Except as provided in this Agreement, Escrow Agent shall not disclose, transfer, make available, or use the Deposit Materials. Escrow Agent shall not disclose the contents of this Agreement to any third party. If Escrow Agent receives a subpoena or other order of a court or other judicial tribunal pertaining to the disclosure or release of the Deposit Materials, Escrow Agent shall immediately notify the parties to this Agreement unless prohibited by law. It shall be the

responsibility of Depositor and Licensee to challenge any such order; provided, however, that Escrow Agent does not waive its rights to present its position with respect to any such order. Escrow Agent shall not be required to disobey any court or other judicial tribunal order.

2.2. *Status Reports.* Escrow Agent shall issue to Depositor and Licensee a report profiling the account history pertaining to this Agreement at least twice per calendar year. Escrow Agent shall provide copies of such account history on the request of any party to this Agreement.

2.3. *Audit Rights.* During the term of this Agreement, Depositor and Licensee shall each have the right to inspect the written records of Escrow Agent pertaining to this Agreement. Any inspection shall be held during normal business hours and on reasonable prior notice to the other parties.

ARTICLE 3: GRANT OF RIGHTS TO ESCROW AGENT

3.1. *Title to Media*. Depositor hereby transfers to Escrow Agent title to the media on which the proprietary technology and materials are written or stored; provided, however, that this transfer does not include ownership of the Source Code or other materials contained on the media or any copyright, trade secret, patent, or other intellectual property rights.

3.2. *Right to Make Copies*. Escrow Agent shall have the right to make copies of the Deposit Materials as reasonably necessary to perform this Agreement. Escrow Agent shall copy all copyright, nondisclosure, and other proprietary notices and legends contained on the Deposit Materials onto any copies made by Escrow Agent. With all Deposit Materials submitted to Escrow Agent, Depositor shall provide all instructions necessary to duplicate the Deposit Materials, including, but not limited to, the hardware and software needed.

3.3. *Right to Transfer on Release*. Depositor hereby grants to Escrow Agent the right to transfer the Deposit Materials to Licensee on any release of the Deposit Materials for use by Licensee in accordance with Section 4.5. Except on such a release or as otherwise provided in this Agreement, Escrow Agent shall not transfer the Deposit Materials.

ARTICLE 4: RELEASE OF DEPOSIT

4.1. *Release Conditions*. As used in this Agreement, "Release Condition" shall mean the following:

(a) Depositor's failure to carry out any obligation relating to delivery or support of the Source Code under the License Agreement, which failure prevents Licensee from obtaining the benefits of or related to the Source Code granted by the License Agreement such that Licensee is not able to perform its obligations under the License Agreement to its customers, and which failure continues for a period of 30 days after Depositor receives written notice of the failure from Licensee;

(b) Depositor's ceasing to conduct its operations pertaining to the Source Code or to the License Agreement in the normal course of business, including, without limitation, any voluntary or involuntary liquidation, dissolution, or winding up of the business of Depositor;

(c) The bringing by or against Depositor of any proceedings under any bankruptcy or insolvency law, which proceedings, if involuntary, shall have not been dismissed within 60 days after the date of filing; or

(d) The appointment or application for appointment of a receiver or the like for Depositor, which is not vacated within 60 days after such appointment or application for appointment.

Comment: Counsel should try to determine all the circumstances where a release of the software would be necessary. This will help prevent loss of the software. Another release trigger event may be the departure of certain important personnel who provide assistance with respect to the deposited materials.

4.2. *Request for Release*. If Licensee believes in good faith that a Release Condition has occurred, Licensee may provide to Escrow Agent written notice of the occurrence of the Release Condition and a request for the release of the Deposit Materials. On receipt of such notice, Escrow Agent shall provide a copy of the notice to Depositor by commercial express mail.

4.3. *Contrary Instructions*. From the date that Depositor receives the copy from the Escrow Agent of the

Licensee's notice under Section 4.2, Depositor shall have 20 business days to deliver to Escrow Agent Contrary Instructions. "Contrary Instructions" shall mean the written representation by Depositor that a Release Condition either has not occurred or has been cured. On receipt of Contrary Instructions, Escrow Agent shall send a copy of the same to Licensee by commercial express mail. Additionally, Escrow Agent shall notify both Depositor and Licensee that there is a dispute under this Agreement to be resolved pursuant to Section 7.3. Subject to Section 5.2, Escrow Agent shall continue to store the Deposit Materials without release pending (a) joint instructions from Depositor and Licensee; (b) resolution pursuant to Section 7.3; or (c) order of a court.

4.4. *Release of Deposit*. If Escrow Agent does not receive Contrary Instructions from the Depositor, Escrow Agent is authorized to release the Deposit Materials to the Licensee; provided, however, that, Escrow Agent is entitled to receive any fees due Escrow Agent before making the release. Any copying expenses in excess of $300 shall be chargeable to Licensee. This Agreement will terminate on the release of all Deposit Materials held by Escrow Agent under Section 4.3 or 4.4.

4.5. *Right to Use Following Release*. Following release of the Deposit Materials in accordance with this Article 4, Licensee shall have the right to use the Deposit Materials for the sole purpose of continuing the benefits afforded to Licensee under the terms and conditions of the License Agreement, including, if necessary, the right to use the Deposit Materials to make (or have made) any items necessary for Licensee to be able to continue any benefits afforded under the terms and conditions of the License Agreement. Licensee shall be obligated to maintain the confidentiality of the released Deposit Materials in accordance with the terms of the License Agreement. Any release of the Deposit Materials to Licensee hereunder shall not relieve any party of any obligations to make any payments to any other party required by the License Agreement.

Comment: Dispute resolution may or may not be the preferred method of resolving differences between the depositor and the licensee as to whether a release event has occurred. If the licensee has more leverage than the depositor, the licensee may instead include a provision requiring the immediate release of the deposited materials upon the licensee's request.

ARTICLE 5: TERM AND TERMINATION

5.1. *Term of Agreement*. Unless sooner terminated under Section 4.4, the initial term of this Agreement is for a period of one year. Thereafter, this Agreement shall automatically renew from year to year unless (a) Depositor and Licensee jointly instruct Escrow Agent in writing that the Agreement is terminated; (b) the Agreement is terminated by Escrow Agent for nonpayment in accordance with Section 5.2; or (c) the Agreement is terminated under Section 4.4. If the Deposit Materials are subject to another escrow agreement with Escrow Agent, Escrow Agent reserves the right, after the initial one-year term, to adjust the anniversary date of this Agreement to match the then prevailing anniversary date of such other escrow arrangements.

Comment: Often a depositor will have several licensees who have requested escrow agreements for the same software program, and the depositor may find itself repeatedly depositing the same deposit materials with its escrow agent to comply with each license agreement. For convenience of administration, the escrow agent may wish to align the various escrow agreements so that they share the same anniversary date. The last sentence of this section permits an escrow agent to do this.

5.2. *Termination for Nonpayment*. In the event of any nonpayment of fees owed to Escrow Agent under this Agreement, Escrow Agent shall provide written notice of delinquency to all parties to this Agreement. Any party shall have the right to make the payment to Escrow Agent to cure the default. If the past due amount is not received by Escrow Agent within 30 days after the date of the delinquency notice, then Escrow Agent shall have the right to terminate this Agreement at any time thereafter by sending written notice of termination to all parties. Escrow Agent shall have no obligation to take any action under this Agreement as long as any payment due to Escrow Agent under this Agreement remains unpaid.

5.3. *Disposition of Deposit Materials on Termination*. On termination of this Agreement, Escrow Agent shall destroy, return, or otherwise deliver the Deposit Materials in accordance with Depositor's instructions, unless the Deposit Materials are released to the Licensee under Section 4.4, in which case the Escrow Agent shall follow any instructions given by the Licensee. If there are no instructions, Escrow Agent may, at its sole discretion, destroy the Deposit Materials or return them to Depositor. Escrow Agent shall have no obligation to return or destroy the Deposit Materials if the Deposit Materials are subject to another escrow agreement with

Escrow Agent.

5.4. *Survival of Terms Following Termination*. On termination of this Agreement, the following provisions of this Agreement shall survive:

(a) Depositor's Representations (Section 1.5);

(b) The obligations of confidentiality with respect to the Deposit Materials;

(c) The rights granted in the sections entitled Right to Transfer on Release (Section 3.3) and Right to Use Following Release (Section 4.5), if a release of the Deposit Materials has occurred prior to termination;

(d) The obligation to pay Escrow Agent any fees and expenses due;

(e) The provisions of Article 7; and

(f) Any provisions in this Agreement that specifically state they survive the termination or expiration of this Agreement.

ARTICLE 6: ESCROW AGENT'S FEES

6.1. *Fee Schedule*. Escrow Agent shall be paid its standard fees and expenses applicable to the services provided under this Agreement, in accordance with the schedule attached hereto as Exhibit C. _ _[*Depositor/Licensee/Depositor and Licensee each*]_ _ shall be responsible for payment of the Escrow Agent's fees and expenses hereunder. Escrow Agent shall notify the party or parties responsible for payment of Escrow Agent's fees at least 60 days prior to any increase in fees. For any service not listed on Escrow Agent's standard fee schedule, Escrow Agent shall provide a quote prior to rendering the service, if requested.

6.2. *Payment Terms*. Escrow Agent shall not be required to perform any service under this Agreement unless the payment for such service and any outstanding balances owed to Escrow Agent are paid in full. Fees are due and payable as set forth on Exhibit C on the Escrow Agent's receipt of a fully executed counterpart of this Agreement or receipt of the Deposit Materials, whichever is earliest. If fees are not paid, Escrow Agent may terminate this Agreement in accordance with Section 5.2. Late fees on past due amounts shall accrue interest at the rate of 1.5% per month (18% per annum) from the date of the invoice.

ARTICLE 7: LIABILITY AND DISPUTES

7.1. *Right to Rely on Instructions*. Escrow Agent may act in reliance on any instruction, instrument, or signature reasonably believed by Escrow Agent to be genuine. Escrow Agent may assume that any employee of a party to this Agreement who gives any written notice, request, or instruction has the authority to do so. Escrow Agent will not be required to inquire into the truth or evaluate the merit of any statement or representation contained in any notice or document received by Escrow Agent. Escrow Agent shall not be responsible for failure to act as a result of causes beyond the reasonable control of Escrow Agent.

7.2. *Indemnification*. Depositor and Licensee agree jointly and severally to indemnify, defend, and hold harmless Escrow Agent from and against any and all claims, actions, damages, demands, fees and expenses (including, without limitation, attorney fees and costs), and other liabilities (collectively, "Liabilities") incurred by Escrow Agent relating in any way to this escrow arrangement unless the Liabilities were caused solely by the negligence or willful misconduct of Escrow Agent; provided, however, that (a) Licensee shall have no obligation under this Section 7.2 with respect to any Liabilities that result solely from or arise solely in connection with an act or omission by Depositor, and (b) Depositor shall have no obligation under this Section 7.2 with respect to any Liabilities that result solely from or arise solely in connection with an act or omission by Licensee.

7.3. *Dispute Resolution*. Any dispute relating to or arising from this Agreement shall be resolved by arbitration under the Commercial Rules of the American Arbitration Association. There shall be three arbitrators. The Depositor and Licensee shall each select one arbitrator, and the two chosen arbitrators shall select the third arbitrator, or, failing agreement on the selection of the third arbitrator, the American Arbitration Association shall select the third arbitrator; provided, however, that if Escrow Agent is a party to the arbitration, Escrow Agent shall select the third arbitrator. Arbitration shall take place in _ _[*city*]_ _, California.

Any court having jurisdiction over the matter may enter judgment on the award of the arbitrator(s). Service of a petition to confirm the arbitration award may be made by First Class mail or by commercial express mail, to the attorney for the party or, if unrepresented, to the party at the last known business address.

Comment: If the deposited materials are very important to the licensee's business, consider adding procedures for expedited arbitration to mitigate against the risk of a protracted dispute.

7.4. *Governing Law.* This Agreement shall be governed and construed in accordance with the laws of the State of California, without regard to its conflict of law provisions.

7.5. *Notice of Requested Order.* If any party intends to obtain an order from the arbitrator or any court of competent jurisdiction that may direct Escrow Agent to take, or refrain from taking any action, that party shall:

(a) Give Escrow Agent at least 2 business days' prior notice of the hearing;

(b) Request that the arbitrator or court include in any such order that, as a precondition to Escrow Agent's obligation, Escrow Agent be paid in full for any past due fees and be paid for the reasonable value of the services to be rendered pursuant to such order; and

(c) Request that the arbitrator or court not require Escrow Agent to deliver the original (as opposed to a copy) of the Deposit Materials if Escrow Agent may need to retain the original in its possession to fulfill any of its other duties.

ARTICLE 8: GENERAL PROVISIONS

8.1. *Entire Agreement*. This Agreement, which includes the Exhibits described herein, embodies the entire understanding among the parties with respect to its subject matter and supersedes all previous communications, representations, or understandings, either oral or written. Escrow Agent is not a party to the License Agreement between Depositor and Licensee and has no knowledge of any of the terms or provisions of the License Agreement. Escrow Agent's only obligations to Depositor or Licensee are as set forth in this Agreement. No amendment or modification of this Agreement shall be valid or binding unless signed by all the parties hereto, except that Exhibit A need not be signed by Escrow Agent, Exhibit B need not be signed by Licensee, and Exhibits C and D need not be signed.

8.2. *Notices.* Whenever notice is to be served hereunder, service shall be made personally, by overnight courier, or by registered or certified mail, return receipt requested, sent or delivered to the parties at the addresses specified in Exhibit D. The party sending the notice shall prepay all postage and other delivery charges. All notices shall be deemed to have been given (a) if by hand, at the time of the delivery thereof to the receiving party at the address of such party set forth above; (b) if sent by overnight courier, then on the next business day following the day such notice is delivered to the courier service; or (c) if sent by registered or certified mail, on the third business day following the day such mailing is made. It shall be the responsibility of the parties to notify each other as provided in this Section 8.2 in the event of a change of address. The parties shall have the right to rely on the last known address of the other parties.

8.3. *Severability.* In the event any provision of this Agreement is found to be invalid, voidable, or unenforceable, the parties agree that unless it materially affects the entire intent and purpose of this Agreement, such invalidity, voidability, or unenforceability shall affect neither the validity of this Agreement nor the remaining provisions herein, and the provision in question shall be deemed to be replaced with a valid and enforceable provision most closely reflecting the intent and purpose of the original provision.

8.4. *Successors.* This Agreement shall be binding on and shall inure to the benefit of the successors and assigns of the parties; provided, however, that Escrow Agent shall have no obligation to recognize any successor or assign of Depositor or Licensee unless Escrow Agent receives clear, authoritative, and conclusive written evidence of the substitution of parties.

8.5. *Regulations.* Depositor and Licensee are responsible for and warrant compliance with all applicable laws, rules, and regulations, including but not limited to, customs laws, import, export, and re-export laws and government regulations of any country from or to which the Deposit Materials may be delivered in accordance with the provisions of this Agreement.

IN WITNESS WHEREOF, the parties have executed this agreement as of the day and year first above written.

Date: _ _ _ _ _ _

_ _[*NAME OF DEPOSITOR*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

Date: _ _ _ _ _ _

_ _[*NAME OF LICENSEE*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

Date: _ _ _ _ _ _

_ _[*NAME OF ESCROW AGENT*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

EXHIBIT A

MATERIALS TO BE DEPOSITED

Depositor represents to Licensee that Deposit Materials delivered to Escrow Agent shall consist of the following. The Deposit Materials are described in greater detail on Exhibit B to this Agreement.

_ _[*List of Deposit Materials*]_ _

EXHIBIT B

DESCRIPTION OF DEPOSIT MATERIALS

Depositor: _ _[*Company name and address*]_ _

Account Number: _ _[*escrow account number*]_ _

Product Name: _ _[*name of product as listed on Exhibit A*]_ _

Version: _ _[*version number*]_ _

(Product Name will appear as the Exhibit B Name on Account History report)

Quantity	**Media Type & Size**	**Label Description of Each Separate Item**
_____	**Disk 3.5" or ____**	_____
_____	**DAT tape ____mm**	_____
_____	**CD-ROM**	_____
_____	**Data cartridge tape ___**	_____
_____	**TK 70 or ____ tape**	_____

_____ Magnetic tape ____ _____

_____ Documentation _____

_____ Other _____ _____

PRODUCT DESCRIPTION:

_____

Environment _____

DEPOSIT MATERIAL INFORMATION:

_____

Is the media encrypted? _ _[*Yes/No*]**_ _ If yes, please include any passwords and the decryption tools.**

Encryption tool _ _[*name, version*]**_ _**

Hardware required _ _[*name*]**_ _**

Software required _ _[*name*]**_ _**

Other required information _____

I certify for Depositor that the above-described Deposit Materials have been transmitted to Escrow Agent:

Date: _ _ _ _ _ _

_ _[*NAME OF DEPOSITOR*]_ _**,**
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

Escrow Agent has inspected and accepted the above Deposit Materials (any exceptions are noted above):

Date: _ _ _ _ _ _

_ _[*NAME OF ESCROW AGENT*]_ _**,**
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

Date Accepted: _ _[*date*]_ _

Send materials to Escrow Agent at:

_ _[*name*]_ _
_ _[*address*]_ _

EXHIBIT C

ESCROW AGENT'S SCHEDULE OF FEES

_ _[*Attach schedule of fees and payment dates*]_ _

EXHIBIT D

DESIGNATED CONTACT NAMES AND ADDRESSES

Notices, deposit material returns, and communications to Depositor should be addressed to: _ _[*depositor contact's address*]**_ _.**

Invoices to Depositor should be addressed to: _ _[*depositor accounts payable address*]**_ _.**

Requests from Depositor or Licensee to change the designated contact should be given in writing by the designated contact or an authorized employee of Depositor or Licensee.

Contracts, Deposit Materials, and notices to Escrow Agent should be addressed to: _ _[*escrow agent address*]**_ _.**

© The Regents of the University of California

16

Financing an Online Business

I. EARLY-STAGE EQUITY FINANCING
- A. Introduction §16.1
- B. Equity Versus Debt
  - 1. Equity §16.2
  - 2. Debt §16.3
- C. Sources of Equity Funding §16.4
  - 1. Founders, Friends, and Family §16.5
  - 2. "Angel" Investors §16.6
  - 3. Venture Capital and Other Institutional Investors §16.7
- D. Structure of Venture Capital Financings §16.8
- E. Venture Capital Financing Term Sheet
  - 1. Introduction §16.9
  - 2. Form: Term Sheet for Preferred Stock Financing §16.10

II. DEBT FINANCING
- A. Introduction §16.11
- B. Types of Debt Financing §16.12
  - 1. Working Capital Loans §16.13
  - 2. Term Loans §16.14
  - 3. SBA Loans §16.15
  - 4. Lease Financings §16.16
  - 5. Corporate Credit Cards §16.17
  - 6. Convertible Debt §16.18
  - 7. Customer Advances §16.19
- C. Qualifying for Loan §16.20
- D. Elements of Simple Loan Transaction
  - 1. Overview §16.21
  - 2. Usury Issues for Non-Bank Lenders §16.22
- E. Loan Agreement and Promissory Note §16.23
  - 1. Form: Loan Agreement §16.24
  - 2. Form: Promissory Note §16.25
- F. Security Interests in Intellectual Property Collateral
  - 1. Generally §16.26
  - 2. Security Interests in Copyrights §16.27
  - 3. Security Interests in Patents §16.28
  - 4. Security Interests in Trademarks §16.29
  - 5. Security Interests in Domain Names §16.30
  - 6. Security Interests in Trade Secrets §16.31
  - 7. Form of Security Agreement (Intellectual Property)
    - a. Introduction §16.32
    - b. Form: Security Agreement (Intellectual Property) §16.33
- G. Convertible Promissory Notes
  - 1. Generally §16.34
  - 2. Form: Convertible Promissory Note §16.35

© The Regents of the University of California

I. EARLY-STAGE EQUITY FINANCING

§16.1 A. Introduction

Sections 16.2-16.35 address ways in which early-stage Internet-based businesses typically obtain funds to pay for development, growth, and operations. Most new Internet companies without a "bricks and mortar" presence have significant ongoing expenses for business development, but have yet to market a product or service and thus are not generating cash. Because of their limited operating history and lack of revenues, these companies cannot access funding sources such as commercial banks that are available to more seasoned companies. Therefore, early-stage companies normally rely on sales of equity interests to finance their activities. Sections 16.2-16.10 focus on the most common sources of equity and the terms that early-stage companies typically encounter when they seek equity financing.

There are inherent tensions between the interests of company founders and the interests of investors. Founders are usually entrepreneurs with an idea, technological skills, and a vision of building a business, running it their own way, and perhaps passing it down to their children. The interests of investors are usually more limited: the highest and quickest return on their money with as little risk as possible. The structure and documentation of equity investments represents a balancing of these often conflicting interests.

For additional discussion of equity financing for start-up companies, see Financing and Protecting California Businesses (Cal CEB 2006). For a comprehensive directory of sources of equity (as well as debt) financing for both early- and later-stage companies, see The Corporate Finance Sourcebook, published annually by the National Register Publishing Company, http://www.financesourcebook.com. Before approaching any financing source, the company should have a well-prepared business plan. For an extensive discussion of business plans, together with checklists and confidentiality agreement forms, see Financing and Protecting California Businesses, chap 2 (Cal CEB 2006).

© The Regents of the University of California

B. Equity Versus Debt

§16.2 1. Equity

Equity represents an ownership interest in the company, and the fortunes of equity investors follow the fortunes of the company. There is no guarantee that equity investors will ever make a return on their investment, or even get their money back. This inherent risk of equity investment, however, comes with a possible upside: If the company is wildly successful, the investors could make a fortune, because they own part of the company.

Equity comes in many forms, depending on the legal structure of the enterprise. For corporations, equity is typically either common stock or preferred stock, but may also take the form of warrants (*i.e.,* an option to buy either common or preferred stock in the future for a fixed price determined today). There are also more exotic or hybrid types of corporate equity, such as convertible preferred stock, limited only by applicable laws and the imaginations of attorneys.

Common stock is the simplest form of corporate ownership interest, and typically gives the holder voting rights on major corporate actions (such as mergers and dissolution), the election of directors, dividend rights, and liquidation rights. See generally Organizing Corporations in California (3d ed Cal CEB 2001); Financing and Protecting California Businesses (Cal CEB 2006). Most stock traded on the stock exchanges and Nasdaq is common stock, and most founders of nonpublic companies hold common stock.

Preferred stock is a more complex form of equity interest and may carry a variety of features. See generally Corp C §§400-403; Financing and Protecting §§5.13-5.18. Nearly all preferred stock will have a liquidation preference, the amount of which may vary from one times the amount of the investor's original investment to 10 times that amount or more. The size of the liquidation preference is largely determined by supply and demand in the venture capital markets —more money chasing fewer good companies results in lower liquidation preferences, and vice versa. Preferred stock may also have conversion features (optional, mandatory, or automatic conversion into common stock on the happening of certain events), redemption features (the ability of the company or the investor to require the company to repurchase the stock), and protective provisions (the ability of preferred shareholders to block certain corporate actions, such as mergers or charter amendments, on an other than "majority-rule" basis). Most venture capital investments in early-stage companies take the form of an investment in preferred stock.

In recent years, the limited liability company (LLC) has become a commonly used form of business entity. See generally Forming and Operating California Limited Liability Companies (2d ed Cal CEB 2007). LLC ownership interests are often designated as "units," and may be common or preferred units, or may be designated by class (*e.g.,* Class A Units, Class B Units) with different classes having different attributes of ownership, akin to common and preferred stock of a corporation. Ownership interests in LLCs may also simply be called "interests," and an investor's share of the company is expressed as a percentage. LLCs offer greater flexibility than corporations in many respects, including allocation of profits and losses and governance rights. The LLC form, however, has some limitations. For example, it is customary for investment bankers to advise an LLC, as a precondition to an initial public offering, to convert to a corporate structure so that investors will not be deterred by cumbersome prospectus disclosures regarding LLC governance, accounting, and tax matters.

Companies may also operate as a partnership, either limited or general, but partnership entities have been used much less frequently since the advent of LLCs. For general information concerning partnerships, see Advising California Partnerships (3d ed Cal CEB 1999).

© The Regents of the University of California

§16.3 2. Debt

The alternative to equity financing for Internet-based businesses is debt, although institutional debt financing is usually not available for early-stage (pre-revenue) companies. For new companies, debt financing usually takes the form of a loan by the founder, a shareholder or other principal, or an "angel" investor. Debt does not convey an ownership interest in the company (although some debt is convertible into equity), but is merely an obligation to repay money over a specified period of time or on a specified date, which bears interest at a specified fixed or variable rate. See §§16.11-16.35 for further discussion of debt financing.

For start-up companies, debt sometimes takes the form of a "bridge" loan from an investor. A bridge loan is a short-term loan, often made while parties are negotiating the terms of an equity investment. As soon as the equity investment is funded, the bridge loan is repaid from the proceeds of the investment. Bridge loans are often used by venture capital firms to provide necessary working capital so that a company can continue to operate while a larger equity financing is completed.

Commercial loans are usually secured by the company's assets, including equipment, real estate (if any), accounts receivable, inventory, and, often most importantly for Internet-based businesses, intellectual property—domain names, software source codes and other copyrighted materials, trademarks, and sometimes patents. Most of the value of an online business may lie in its intellectual property. If the company defaults on its secured debt, the lender can foreclose on the loan collateral, and the company's shareholders may lose their entire investment.

If a company has a willing lender, debt financing may be preferred by entrepreneurs who do not want to give additional equity ownership interests to outsiders. Unlike equity, however, debt must be repaid within a certain time frame and, if the lender requires personal guaranties from the founders, carries personal exposure for the founders that would not be present in a typical equity offering. If a company does not have sufficient funds to repay secured debt on time, company assets may be lost to a foreclosing lender. Thus, debt is often more risky from the viewpoint of the company's founders.

© The Regents of the University of California

§16.4 C. Sources of Equity Funding

Equity funding for Internet-based businesses may come from a variety of sources, depending on the company's stage of development and need for funds. A start-up company with "just an idea" has different needs than a software company preparing to launch a beta test. Both of these companies have different needs than a company embarking on a national product roll-out. At each stage of a company's development, different types of investors may be more or less willing to make an equity investment.

Throughout the life of an enterprise, two basic principles govern: (1) access to capital facilitates growth, and (2) those providing capital often demand ownership and, depending on the amount of capital furnished, control. These principles often conflict, and must be appropriately balanced for all parties to be satisfied. For an entrepreneur to grow the company, he or she must have funding, but to get more money, at least in the pre-revenue stage and often afterwards, he or she must give a greater share of the company to investors and will thereby have less control over the company's fate.

These conflicts may figure prominently when contemplating what are commonly referred to as "exit strategies." An exit strategy simply means, "how and when do I get my money back?" An entrepreneur may envision the company as a long-term proposition, one that he or she intends to operate indefinitely, sometimes for a lifetime. Investors, on the other hand, usually want to be able to take their money out sooner, receive a return on their investment, and move on, either through a sale of the company, a public offering, new debt financing, or another means of providing liquidity. Thoughtful design of the enterprise's capital structure often determines whether everybody wins or whether some people lose in this conflict.

© The Regents of the University of California

§16.5 1. Founders, Friends, and Family

Many start-up companies are financed initially with personal funds of the founders and their relatives and friends. This seed capital may range from a few thousand to a hundred thousand dollars or more, depending on the business's needs and the founders' circle of acquaintances, and may be used for start-up expenses, infrastructure building, or day-to-day operations.

The interests of the founder and "friends and family" investors are typically more closely aligned than those of the founder and later-stage investors such as venture capital firms. Equity capital from friends and family usually comes without many strings attached; friends and family members usually purchase common stock and often are not interested in taking part in the day-to-day operations of the company. This often coincides nicely with the founder's desire to run the company his or her own way. One major legal risk associated with friends and family investors, however, is that they may lack sophistication in financial and business matters, and as a result, careful attention must be paid to assuring that there are appropriate exemptions from the requirement to register the stock offering under federal and state securities laws. See generally Financing and Protecting California Businesses, chap 6 (Cal CEB 2006).

For start-up companies, there are no hard-and-fast rules concerning the proportion of equity ownership received in return for an initial equity investment. Often, the founder or founders will contribute the idea, personal services ("sweat equity"), intellectual property (such as proprietary source code), and some amount of cash, in exchange for common stock. Control of the company is important to founders, and, in a simple corporate structure, the founders normally wish to retain ownership of at least 51 percent of the voting stock. Other key factors include the relative leverage or bargaining positions of the founders and the initial cash investors, and the valuation (or the parties' perception of the valuation) of the founders' noncash contributions to the company.

In valuing founders' contributions, founders usually start with the advantage that, without their talents and knowledge (and in-kind contributions such as intellectual property), the company would not exist or have a chance to succeed. Thus, the founders' ownership interests are usually out of proportion to the amount of cash (if any) that they actually invest. If an initial investor, for example, receives a 5-percent interest in the company for an investment of $20,000 in cash and the founders retain 95 percent, the company's total value is theoretically $400,000, with the founders' contributions theoretically worth $380,000.

Earlier valuations will influence later valuations. If, one year later, the company wishes to sell another 5 percent to a second investor for $1 million, the company will have to show reasons—such as increased sales, completed beta testing, or an established distribution network—why 5 percent is now worth so much more than $20,000.

These examples should not be interpreted as a guide to the percentage of stock that should be given to outside investors or retained by the founder. They are merely intended to illustrate how valuation concepts work in practice.

PRACTICE TIP: A common but unfortunate tendency for many start-up companies is to ignore the corporate formalities necessary to properly document the initial investments by founders, friends, and family to save on legal fees. Proper documentation and observance of other corporate formalities—including federal and state securities law compliance—is always essential, but especially in hindsight, at later stages of a company's life, when corporate opportunities present themselves or interpersonal relationships among the principals change. At that point, problems resulting from improper documentation may be resolvable only in litigation or otherwise at significant extra legal expense. Moreover, the failure to properly document early-stage equity transactions and ensure securities law compliance may impair the company's ability to secure later-stage financing or attract merger or acquisition candidates.

© The Regents of the University of California

§16.6 2. "Angel" Investors

So-called "angel" investors often provide the next stage of funding in the life of Internet-based businesses. Angel investors are usually high net-worth individuals, trusts, or other entities, sometimes professionals, with capital to wager on more risky early-stage companies and a desire to be a part of the introduction of innovative technologies. Angels usually do not want to be involved in the day-to-day operations of the business, but may wish to hold seats on the board of directors. They may be willing to assume more risk and make smaller investments than a venture capital fund. There are also organizations of angel investors, who investigate opportunities jointly and may invest individually or as a group. See, *e.g.,* http://www.garage.com. There are several online directories of angel investors. See, *e.g*., http://www.angel-investor-network.com/.

© The Regents of the University of California

§16.7 3. Venture Capital and Other Institutional Investors

Venture capital firms, hedge funds, strategic partners (*i.e.,* larger, established companies with complementary businesses such as software distributors or Internet service providers), and other institutional investors often follow angel investors into companies that are demonstrating success or a strong potential for success. Each institution establishes its own policies for the type and quality of its investments. One firm may invest from $1 million to $3 million in software companies at the beta-test stage. Another may invest $10 million to $20 million in Internet companies at the revenue stage. Some firms want to play a "hands on" role in management, while others are content with a more passive approach. As noted in §16.2, venture capital firms commonly invest in preferred stock, although some provide bridge financing or convertible debt. They frequently desire an "exit" within 5 to 7 years, although strategic-partner investors may be longer-term players.

The requirements of venture capital investors often conflict with the desires of entrepreneurs. Providing access to capital gives venture capital firms significant bargaining power. Venture capital transactions are often heavily negotiated and result in complex capital structures. Moreover, early-stage investors and the founders themselves often must relinquish some control and have their ownership diluted as a condition of the venture capital financing. It is part of company counsel's role to help ensure that transactions with venture capital investors are as fair to the company and existing shareholders as possible.

© The Regents of the University of California

§16.8 D. Structure of Venture Capital Financings

Although investment structures are continually evolving, many venture capital and institutional financings have common elements with which the practitioner should be familiar. At the start of most venture capital and institutional financings, a term sheet is negotiated, which provides the framework around which more detailed transactional documents are constructed. Section 16.10 sets forth the basic elements of a first-round venture capital financing term sheet with commentary intended to highlight some issues that arise in structuring a venture capital investment. While investments by strategic partner-investors often have a similar structure to venture capital investments, they also involve other business relationships that must be negotiated and documented. Strategic relationships are discussed in chap 11.

Venture capital investments in the form of preferred stock may be made over a period of time, with each successive round of investment denominated alphabetically, *e.g.,* Series A Preferred Stock, Series B Preferred Stock. Often, each successive series has greater rights than the previous series, and, if the company's performance is improving, is at a greater valuation. If the company is not performing as expected, subsequent financings may still occur, but at a lesser valuation. Such a "down round" results in a greater percentage of the company being sold for a smaller investment, often diluting the investment of earlier investors.

Venture capital financing transactions are complex and heavily documented. Typical documents and agreements that are drafted and negotiated by counsel include:

- **Stock Purchase Agreement.** The basic agreement under which the shares are purchased, it includes representations, warranties, and covenants of the company and investors.
- **Amended and Restated Articles of Incorporation.** Filed by the company immediately before closing, this document sets forth the internal "law" of the corporation and the fundamental terms of the preferred stock being issued.
- **Investor Rights Agreement.** This document sets forth additional rights of investors, such as registration rights, that are not included in the articles.
- **Shareholders' Agreement.** This agreement among shareholders and the company may contain co-sale rights, rights of first refusal, share purchase and repurchase options exercisable on specified events, and agreements to vote for investors' nominees. Agreements regarding shareholder voting may be placed in a separate voting agreement.
- **Management Employment Agreements.** These contracts are often required by investors to ensure that management will stay around to operate the company.
- **Proprietary Information and Inventions Agreement.** This agreement is the main form of protection of the company's intellectual property in relation to its employees (including management), and is usually required by venture investors to protect their investment.
- **Vesting Agreements.** These agreements allow the company to repurchase management's stock if their employment terminates before a prescribed date, and also used to ensure that management stays with the company.
- **Market Stand-Off Agreements.** Insiders who hold common stock are often required to sign market stand-off agreements to restrict their ability to sell shares during or for a specified period of time after a public offering, to avoid depressing the market price of the newly offered shares.
- **Opinion of Counsel.** Opinions of company counsel, covering a variety of legal issues affecting the company, are usually required by venture investors.

Depending on its complexity, the transaction may require additional agreements and documents. For sample forms of some of the documents listed above, see Financing and Protecting California Businesses (Cal CEB 2006). See also the set of model venture capital financing documents promulgated by the National Venture Capital Association, available for downloading at http://www.nvca.org/model_documents/model_docs.html.

Legal fees can be a factor for the company in deciding whether to undertake a venture capital financing. If fees are very large, outside counsel for the company may require that it be paid out of the proceeds of the offering at closing. Some typical provisions of venture capital financing documents are discussed in §§16.9-16.10.

© The Regents of the University of California

E. Venture Capital Financing Term Sheet

§16.9 1. Introduction

The model term sheet in §16.10 is for a simple initial Series A Preferred Stock financing. Venture capital transactions vary in complexity, and this term sheet includes only representative terms. For another form of term sheet for a preferred stock offering, see Financing and Protecting California Businesses, chap 7 (Cal CEB 2006).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/16 Financing an Online Business/§16.10 2. Form: Term Sheet for Preferred Stock Financing

§16.10 2. Form: Term Sheet for Preferred Stock Financing

To download **Word** version, right click and choose *Save Target As*

To download **WordPerfect** version, right click and choose *Save Target As*

SUMMARY OF DRAFT TERMS
XYZ CORPORATION

_ _[*Date*]_ _

This term sheet summarizes the principal terms of the Series A-round venture capital financing of XYZ Corporation (the "Company"). The Company was incorporated in California on _ _[*date of incorporation*]_ _.

PARTIES; SECURITY

Investors	_ _[*List of investors*]_ _
Security	**Series A Convertible Preferred Stock of XYZ Corporation ("Series A Preferred").**
Price per share	_ _[*Dollar amount*]_ _ **("Original Issue Price").**
Aggregate proceeds	_ _[*Dollar amount*]_ _ **(minimum proceeds required for initial closing).** *Comment:* This amount may be structured as a range (*e.g.,* "a minimum of $6 million and a maximum of $12 million").
Expected closing date	_ _[*Date*]_ _ **(the "Closing Date").** *Comment:* This date is usually provided as a goal. If there is a strict deadline, it should be set forth as, *e.g.,* "In no event later than December 31, 20__."

TERMS OF SERIES A PREFERRED STOCK

Dividend provisions	**Annual _ _[*percent*]_ _% per share dividend on the Series A Preferred. Dividends payable if, as, and when determined by the Board of Directors ("Board"). Dividends are not cumulative. For any other dividends or distributions, Preferred Stock participates with Common Stock on an as-converted basis.** *Comment:* Dividend rates often reflect the prevailing interest rates in the economy (*i.e.,* one to two percentage points above prime). Note that dividends are only payable when the board determines, and are rarely paid in start-up companies.
Liquidation preference	[*Add one of the following alternatives*] [*Alternative 1: Nonparticipating Preferred]* **First pay original purchase price plus accrued dividends on each share of Preferred Stock, then pay balance of proceeds to Common Stock.**

Comment: In any liquidation, the preferred holders will get their money out first, before common holders get anything. Nonparticipating preferred is more favorable for the company, because once preferred holders receive the amount of their original investment, common holders share equally in the remaining proceeds of any sale or liquidation of the company.

[*Alternative 2: Participating Preferred*]

Participating Preferred: First pay original purchase price plus accrued dividends on each share of Preferred Stock, with remaining proceeds paid pro rata to Preferred and Common Stock on an as-converted basis.

Comment: This provision favors the preferred holders over common holders, because preferred investors will receive both their liquidation preference and a portion of any remainder, based on their pro rata ownership interest.

[*If applicable, add the following option*]

A consolidation or merger of the Company or sale of all or substantially all of its assets shall be deemed to be a liquidation or winding up for purposes of the liquidation preference.

[Continue]

Comment: This provision is often included; it allows preferred holders to receive a share of the merger consideration (*i.e.,* stock or cash) equal to their liquidation preference in the event of a merger. Other provisions that effectively give a veto power over mergers to preferred holders are also used, depending on the respective leverage of the parties.

[*Continue*]

Redemption

[*Add one of the following alternatives*]

[*Alternative 1: No Redemption*]

The Preferred Stock shall not be redeemable.

[*Alternative 2: Original Purchase Price Redemption*]

Starting 5 years from the Closing Date, the Series A Holders shall have the right, by majority vote, to require the Company to redeem all of the shares of Series A Convertible Preferred Stock. The redemption price shall be equal to the original purchase price plus accrued dividends. The definitive agreements shall contain remedies for the Investors in the event of a default with respect to the redemption of the Series A Convertible Preferred Stock.

Comment: There are a wide variety of ways

that redemptions can be structured. The form of redemption provision often depends on the relative bargaining power of the parties. Only two examples are given here. Another variation allows the company to elect to redeem or call the shares, often after 7 years. This variation is favorable to the company but is often resisted by investors because it can eliminate their ability to share in future growth of the company.

[*Continue*]

Conversion

Convertible at any time at option of holder into one share of Common Stock (subject to antidilution adjustments).

Comment: Although preferred stockholders are often given optional conversion rights in venture deals, there is usually little incentive for preferred investors to convert to common, at least in the early years, because they would lose the preferences of their preferred stock.

Automatic conversion

The Series A Preferred shall be automatically converted into Common, at the then applicable conversion price, (1) in the event of an underwritten public offering of shares of the Common at a per share not less than _ _[*dollar amount*]_ _ and an aggregate offering price of at least _ _[*dollar amount*]_ _ ("Qualifying IPO") or (2) the date on which the Company obtains the vote or consent of at least 66-2/3% of the then outstanding shares of Series A Preferred Stock approving such conversion.

Comment: Automatic conversion is used at the time of an IPO to simplify the company's capital structure at the initial public offering stage, and is typically required by underwriters. The voting alternative allows a majority to force other holders into a common stock position, often for down rounds in order to avoid a large antidilution adjustment.

Antidilution provision

The Series A Preferred Stock shall be entitled to proportional antidilution protection for stock splits, stock dividends, and the like. In addition, the Investors shall have standard weighted average antidilution rights if the Company issues additional equity securities (other than the reserved employee shares described under "Employee Pool") at a purchase price less than the applicable conversion price.

Comment: Antidilution is designed to protect investors from the diminution in value of their stock that can result from later stock issuances in a down round. There are several varieties of weighted-average antidilution provisions, including narrow-based and broad-based, which exclude different categories of issuances from the

antidilution provisions. Investors favor more narrow-based provisions because they exclude fewer types of issuances. The type of antidilution provision used is a function of the parties' bargaining power.

Voting and protective provisions

Series A Preferred votes on an as-converted to Common basis. In addition, a 2/3 majority vote of the Series A Preferred shall be required for:

(1) Altering, changing, or amending the rights, preferences, and privileges of Series A Preferred Stock;

(2) Authorizing, creating, and/or issuing any senior or pari passu class or series of equity securities, other than an issuance under the existing Employee Pool or conversion of any of the Company's outstanding debt to equity;

(3) Engaging in any business other than the business engaged in by the Company at the time of the Closing;

(4) Increasing or decreasing the authorized number of directors constituting the Board of Directors;

(5) Any consolidation, sale, or merger of the Company or other transaction in which control of the Company is transferred;

(6) Amending or waiving any provision of the Company's Certificate of Incorporation or Bylaws;

(7) Redeeming, repurchasing, or declaring a dividend with regard to any security of the Company prior to _ _[*date*]_ _, except for the Company's repurchase of stock granted under a stock benefits plan.

Comment: These protective provisions give the preferred holders some element of control over the company's activities. The examples listed above are the most common, but parties often negotiate additional provisions suited to their needs.

TERMS OF INVESTOR RIGHTS AGREEMENT

Right of first offer on subsequent issuances

The holders of Preferred Stock shall have the right, if the Company proposes to offer equity securities to any person (other than the securities issued under employee benefit plans or acquisitions, in each case as approved by the Board of Directors, including the director elected by holders of the Series A Preferred), to purchase all or any portion of such shares on a prorata basis. Any securities not subscribed for by an Investor may be reallocated among the other Investors. If the Investors do not purchase all of the securities, the portion that is not purchased may be

offered to other parties on terms no less favorable to the Company for a period of 60 days. This right shall terminate immediately before (1) the closing of a Qualifying IPO; or (2) the closing of any merger or consolidation of the Company.

Comment: This preemptive right gives investors the option to maintain their proportionate interest in the company if the company sells new equity. It can have the effect of preventing new, and perhaps more company-friendly, investors from investing.

This right shall not apply to the issuance by the Company of up to _ _[*number*]_ _ shares of its Common Stock to employees, officers, or directors of, or advisors or consultants to, the Company under its stock purchase or option plans. It shall also not apply to stock issued in connection with strategic alliances or other partnering arrangements approved by the Board of Directors.

Comment: This clause allows the company some leeway to compensate employees and enter into certain types of transactions in which it may want to issue stock without triggering preemptive rights. The scope of the exclusions from preemptive rights are negotiated by the parties, and become another means of investor control.

Registration rights

Comment: Registration rights provide a theoretical exit for investors later in the life of the company. After the company has gone public, the investors can, in specified instances, require the company to register investor shares (demand rights) or can sell shares along with the company the next time the company has a public offering (piggyback rights). There are a number of variations in the terms of these registration rights. The two most common are presented below.

Demand rights

Beginning 6 months after initial registration, two demand registrations on initiation of Investors holding at least 50% of the outstanding shares of Preferred Stock as a class, including Common Stock issued on conversion of the Preferred Stock ("Registrable Securities"), with minimum aggregate offering price to the public of not less than $5,000,000. The Company shall have the right to delay such registration under certain circumstances for two periods not exceeding 90 days each in any 12-month period.

Company registration

Unlimited "piggyback" registration rights subject to prorata cutback at the underwriters' discretion, following initial public offering. If the Investors are limited by cutback, however, no party shall sell shares in such registration other than the Company or the Investors, if

	any, invoking the demand registration.
Termination of registration rights	**Registration Rights terminate (1) 5 years after initial public offering; or (2) when all shares held by an investor can be sold under Rule 144 within a 90-day period.** *Comment:* This provides the company a way to reduce an accumulating number of registration obligations, which usually must be waived to permit new rounds of financing. **No future registration rights may be granted without consent of a majority of Investors holding registration rights unless such rights are subordinate to those of the Investors.**
Expenses	**The Company shall bear registration expenses (exclusive of underwriting discounts and commissions) of all such demand and piggyback registrations (including the expense of one special counsel of the selling shareholders).** *Comment:* Unless the company has significant bargaining power against the investor, the company typically pays all registration expenses.
Standoff provision	**No Investor shall sell shares within 180 days of the effective date of the Company's initial public offering if all officers and directors are similarly bound.** *Comment:* Although venture capitalists may argue against this provision, it is usually required by investment bankers.
Board representation and meetings	**The authorized number of directors shall initially be** **_ _**[*Number*]**_ _, with _ _**[*number*]**_ _ directors elected by the Series A Preferred (voting as a class) and** **_ _**[*Number*]**_ _ directors elected by the Common (voting as a class). Effective on the closing of the Series A Preferred Stock financing, the members of the Board shall be _ _**[*list of names*]**_ _.** *Comment:* Board size and composition are key issues in venture capital financings because of the board's authority over the company's direction and operations, including future financings. Control over the size and composition of the board is typically effected through a voting or shareholders' agreement. Most venture capital investors require at least one board seat, and often more. The board of directors usually acts by majority vote.
Inspection and information rights	**All Investors holding at least _ _**[*number*]**_ _ shares of Preferred Stock shall receive annual audited and quarterly unaudited financial**

statements. 30 days before the start of each fiscal quarter, the Company shall provide to such Investors a comprehensive operating budget forecasting the Company's revenues, expenses, and cash position on a month-to-month basis for the upcoming fiscal quarter. Similar projections shall be provided for the entire fiscal year 60 days before the start of the fiscal year.

TERMS OF PREFERRED STOCK PURCHASE AGREEMENT

Representations and warranties

The investments shall be made under a Stock Purchase Agreement reasonably acceptable to the Company and the Investors, which shall contain, among other things, appropriate representations, warranties, and covenants of the Company reflecting the provisions of this term sheet and other customary provisions, and appropriate conditions to closing including a customary legal opinion of Company counsel regarding the financing.

Comment: Typical representations and warranties of the company include: organization and good standing; capitalization; corporate power and authority; outstanding indebtedness and liabilities; subsidiaries; litigation; proprietary information agreements with employees; intellectual property; material contracts and commitments; financial statements; registration rights; shareholder agreements; employee compensation and pension plans; disclosure and business plan; outstanding securities; and use of proceeds.

Expenses

The Company and the Investors shall each bear their own legal and other expenses with respect to the transaction except that, assuming a successful completion of the transaction, the Company shall pay the legal fees and expenses of _ _[*name*]_ _, counsel to the Investors, up to a maximum of _ _[*dollar amount*]_ _ plus expenses.

Comment: This requirement is typical and increases the cost of a financing to the company. The amount of the investors' fees that the company will be required to pay is the subject of negotiation, and can depend on the size of the investment and the amount of due diligence required. Companies that have kept impeccable records since inception may be able to negotiate this amount downward.

FOUNDERS AND EMPLOYEE AGREEMENTS

Stock vesting

All stock and stock equivalents issued after the Closing to employees, directors, and consultants shall be subject to vesting as follows: 25% to vest at the end of the first year following such issuance, with the remaining 75% to vest monthly over the next 3

	years. The repurchase option shall provide that on termination of the shareholder's employment, with or without cause, the Company or its assignee (to the extent permissible under applicable securities law qualification) retains the option to repurchase at cost any unvested shares held by such shareholder.
Restrictions on Common Stock transfers	**No transfers are allowed before full vesting, subject to certain customary exceptions. The Company shall have a right of first refusal on vested shares until initial public offering.**
Market standoff	**Holders of Common Stock and options must, at the request of the Company or an underwriter involved in the Company's initial public offering, agree not to sell or otherwise transfer any securities of the Company during a period of up to 180 days following the effective date of the registration of such initial public offering.**
Proprietary information and inventions agreement	**Each officer, employee, and consultant of the Company shall enter into a proprietary information and inventions agreement reasonably satisfactory to the Series A Preferred holders.**
Key-man insurance	**As soon as reasonably possible after the Closing, the Company shall procure a key-man life insurance policy for its CEO in the amount of $1,000,000, naming the Company as beneficiary.** *Comment:* Although not always required, a key-man insurance provision is typical in early rounds, when the loss of key individuals could ruin the company's prospects.
Drag-along requirement	**All non-Investor major shareholders will be subject to a requirement that, if the holders of Series A Preferred propose to enter into a merger, sale of assets, or other change of control transaction, and such transaction has been approved by Company's Board of Directors (with the directors appointed by the Series A Preferred voting in favor), such non-Investor holders will be required to take such action as may be required to effect such transaction, including voting their shares in favor of such transaction.** *Comment:* Drag-along rights may vary depending on the leverage of the shareholder group to be dragged along. The drag-along provisions must be designed to coincide with the protective provisions discussed above.
Co-sale rights	**Each holder of the Series A Preferred Stock shall have the right to participate on a prorata basis in any transfers of stock for value by any Founder.** *Comment:* This typical provision is designed to

prevent founders from selling out early and leaving the investors with a shell company.

OTHER PROVISIONS

Expiration

If not accepted by the Company by the close of business by _ _[*date*]_ _, this term sheet shall expire at that time.

Closing conditions

Closing subject to negotiation of definitive legal documents and completion of legal and financial due diligence by Investors.

Capitalization

On the Closing of this financing, there shall be _ _[*number*]_ _ shares of issued and outstanding Common Stock held by the common holders, _ _[*number*]_ _ shares of Common Stock reserved for issuance pursuant to outstanding options or warrants, and an additional _ _[*number*]_ _ shares of Common Stock reserved for future issuance to key employees.

Comment: This condition to the financing is designed to prevent founders from issuing additional stock just before funding, thus diluting the investors' interest.

Nonbinding

This term sheet represents an understanding in principle only, and no party shall be bound with respect to the transactions described herein unless and until definitive agreements shall have been executed by the parties reflecting the terms hereof.

Comment: In most cases, term sheets are not intended to be binding, but serve only as an outline from which to construct final agreements. If, however, there are confidentiality provisions in the letter of intent that usually accompanies a term sheet, those provisions are usually made binding on the parties.

© The Regents of the University of California

II. DEBT FINANCING

§16.11 A. Introduction

Sections 16.12-16.19 review various types of debt financing vehicles that may be available to Internet-based businesses. As discussed in §16.20, qualification for debt financing is an issue for many fledgling Internet companies. A new Internet business may not have financeable inventory and may not generate significant receivables in its early stages while developing its website. The only asset that the business may have to collateralize a loan may be its intellectual property, which may have only a speculative value. If a willing institutional lender can be found, personal guaranties from the founders and principal shareholders are nearly always required. Often, the only willing lenders will be the founders and principal shareholders.

Sections 16.21-16.22 review the basic elements of a loan transaction. Model forms of a loan agreement and promissory note, suitable for a noninstitutional lender, are provided in §§16.23-16.25. Security interests in intellectual property collateral are discussed in §§16.26-16.31; a model form of security agreement is provided in §§16.32-16.33. Unsecured convertible promissory notes have become popular vehicles for financing start-up businesses by angel investors or friends and family members. Convertible notes are discussed in §16.34; a model form is provided in §16.35.

© The Regents of the University of California

§16.12 B. Types of Debt Financing

Debt financing may take many different forms, some of which are discussed in §§16.13-16.19. Start up companies without cash flow may find it difficult to secure debt financing from institutional sources unless they have hard assets to provide as security or the net worth of the founders supports a meaningful guaranty to the lender. Even noninstitutional lenders may insist on some collateral security or a guaranty for the loan.

© The Regents of the University of California

§16.13 1. Working Capital Loans

Working capital loans, also known as operating loans or lines of credit, are typically used to finance a company's day-to-day operations. The loan amount may fluctuate daily based on the cash-flow needs of the company and the value of the collateral. The borrower makes periodic interest payments, and the outstanding principal is due and payable in full at the end of the loan term (sometimes by conversion to a term loan). The lender sets a maximum amount that the company can borrow, typically based on a percentage of the borrower's current accounts receivable (and, if applicable, inventory) balance. Therefore, to qualify for a working capital loan, an Internet business must be generating cash and accounts receivable, and the cash and accounts receivable (and inventory, if applicable) will constitute collateral security for the loan.

© The Regents of the University of California

§16.14 2. Term Loans

A term loan is a loan for a fixed principal amount, usually funded in full on closing of the loan, that is repayable in regular installments of principal and interest. The outstanding principal balance of the loan therefore decreases as loan payments are made over time. Term loans are often used to finance the purchase of long-term assets such as servers and computer equipment, which in turn constitute security for the loan. Equipment acquisition loans typically have an amortization period that matches the useful life of the equipment purchased.

© The Regents of the University of California

§16.15 3. SBA Loans

The Small Business Administration makes direct loans and provides loan guaranties to qualified small businesses that are unable to obtain loans without SBA assistance. 13 CFR §§120.2, 120.100-120.102. Personal guaranties by the business principals and collateral security (in the form of hard assets such as real estate or equipment) are generally required. 13 CFR §§120.150-120.160. For further information concerning the SBA loan program and other SBA programs, see Financing and Protecting California Businesses §§1.11-1.14 (Cal CEB 2006) and the SBA's website, http://www.sba.gov.

© The Regents of the University of California

§16.16 4. Lease Financings

An alternative to borrowing funds to purchase equipment and computer systems is to acquire them through an equipment lease transaction. Leasing rather than buying equipment may offer significant tax, accounting, and operational benefits to a start-up company. The equipment vendor typically has a preexisting relationship with a financial institution that advances funds to acquire the equipment and serves as lessor under the lease. Equipment leases are classified as either capital leases (finance leases) or operating leases (true leases) for tax and accounting purposes. For further discussion of equipment leasing, see Financing and Protecting California Businesses, chap 10 (Cal CEB 2006).

© The Regents of the University of California

§16.17 5. Corporate Credit Cards

Corporate credit cards are unsecured lines of credit, issued in the name of the business for use by authorized employees. Credit cards have the obvious disadvantages of higher interest rates and lower credit limits than conventional loan facilities, but can be useful to meet short-term business needs. If the company has other debt to the issuing institution, credit card obligations are usually treated as part of the company's total loan balance under any guaranty or other security documents for the other debt.

© The Regents of the University of California

§16.18 6. Convertible Debt

Convertible debt is a debt obligation that can be exchanged for a specified amount of equity securities at a later time at the option of the issuer or the holder, or on the happening of certain contingencies. For further discussion of convertible debt and a model form of convertible promissory note, see §§16.34-16.35.

© The Regents of the University of California

§16.19 7. Customer Advances

Structuring the company's business model to create opportunities for advance payments by customers or business partners is another potential source of short-term financing. If the company performs services, licenses intellectual property, or sells goods to third parties, obtaining some portion of the payment in advance will provide interim cash for operating expenses.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/16 Financing an Online Business/§16.20 C. Qualifying for Loan

§16.20 C. Qualifying for Loan

As noted in §16.11, qualifying for a loan may be difficult for a start-up company without inventory or other collateral to secure the loan or a history of cash flow to help ensure repayment. Qualification criteria may include:

- Management expertise;
- A strong business and marketing plan with coverage of the financial aspects of the plan;
- A multi-year history of financial performance reflected in the company's financial statements;
- The ability to repay the loan through business cash flow or the personal means of the principals; and
- Availability of additional security in the form of company-owned hard assets (such as equipment, inventory, receivables, or real estate) or founder guaranties that are also be secured (*e.g.,* by real estate, securities, or cash deposits held by the founders).

As part of their strategic business planning, new Internet-based businesses should take advantage of any opportunity to maximize the potential of meeting lenders' criteria for lending. A company should investigate the lending criteria used by local banks and develop banking relationships by consolidating accounts and credit cards. A company's ability to qualify may increase if the bank links its relationship with the company together with a preexisting relationship with one or more of the company's principals.

© The Regents of the University of California

D. Elements of Simple Loan Transaction

§16.21 1. Overview

A basic loan transaction with a financial institution has several elements, which will vary depending on the identity of lender, the complexity of the transaction, the dollar amount involved, and the security for the loan.

- **Loan application.** Financial institutions have their own forms of loan application and may specify a preferred format for presentation of financial information.
- **Loan agreement.** The loan or credit agreement establishes the basic terms of the loan, and includes representations and warranties by the borrower concerning its business and financial condition and covenants of the borrower regarding its business operations while the loan is outstanding. The loan agreement also includes provisions covering events of default, the lender's remedies on default, and termination of the agreement.
- **Promissory note.** Many financial institutions require borrowers to execute a promissory note as well as the loan agreement, although a separate note is arguably unnecessary because the borrower's legal obligation to repay is also reflected in the loan agreement itself. For small unsecured loans by noninstitutional lenders, a promissory note may be the only documentation of the loan transaction.
- **Security agreement; deed of trust.** If the loan obligation is secured by personal property, including intellectual property, the borrower must execute a security agreement. See generally §§16.26-16.33. A deed of trust is required if the loan collateral includes California real estate. See generally California Mortgages, Deeds of Trust, and Foreclosure Litigation (4th ed Cal CEB 2009).
- **UCC-1 financing statements.** If the loan is secured by personal property, a UCC-1 financing statement must normally be filed to perfect the security interest created by the security agreement. Intellectual property collateral may also require filings in the U.S. Patent & Trademark Office or the U.S. Copyright Office. See §§16.26-16.33.
- **Guaranties.** Institutional lenders often require founders and principals to provide personal guaranties of a company's loan obligations. If the company defaults on the loan, the guaranty permits the lender to seek payment from the guarantor. Guaranties can be joint and several, so that each guarantor is responsible for the entire amount of the loan, or can be structured so that liability under the guaranty is pro rata according to each guarantor's interest in the company or share of distributable profits. Guaranties may be secured or unsecured.
- **Legal opinion.** Financial institutions usually require an opinion of the borrower's counsel on matters including the valid organization and good standing of the borrower and the enforceability of the loan documents. Obtaining a legal opinion from outside counsel can be costly and time-consuming, especially if counsel does not have an in-depth knowledge of the company's legal, operating, and financial history. The cost of a legal opinion should be included in estimating the transaction costs for a loan.

© The Regents of the University of California

§16.22 2. Usury Issues for Non-Bank Lenders

If the lender is not a bank or other institution that qualifies for the California usury exemptions available to financial institutions (see, *e.g.,* Cal Const art XV §1; CC §1916.1; Fin C §§1716, 22002), the lender must ensure that the loan does not violate the California usury law. Unless a statutory exemption is applicable, the maximum permissible interest rate on business loans in California is a rate not exceeding the higher of (a) 10 percent per annum, or (b) 5 percent per annum plus the discount rate charged by the Federal Reserve Bank of San Francisco for advances to its member banks. The rate is measured at the earlier of the time the loan contract is executed or the time the loan is made. Cal Const art XV §1. As of March 1, 2004, the discount rate was 2 percent; the current discount rate can be found online at http://www.frbsf.org/banking/data/discount.

There are three possible usury exemptions that may be available to nonbank business lenders in California. The first, under Corp C §25116(a), covers notes that are either qualified or exempt from qualification under the California state securities laws. See generally Financing and Protecting California Businesses §§6.32-6.42 (Cal CEB 2006). To take advantage of this usury exemption, many practitioners utilize the limited offering securities-law exemption of Corp C §25102(f) (assuming the lender qualifies) and file a Notice of Transaction under 10 Cal Code Regs §260.102.14. The limited offering exemption does not contain any dollar limitations, although it is subject to a 35-purchaser limit. Provided the lender has the requisite sophistication or preexisting relationship with the company or its principals (see Corp C §25102(f)(2)), the loan can be in any amount, and there are no net worth requirements applicable to the borrower.

The second usury exemption, under Corp C §25118(a), is a blanket exemption for notes issued by borrowers with assets of at least $2 million according to their most recent financial statements. The third usury exemption, under Corp C §25118(b), is also a blanket exemption for a note or series of notes aggregating at least $300,000 in face amount at the time of issuance. Both of these usury exemptions require either (a) that the lender and the borrower (or the guarantor) have a preexisting personal or business relationship, or (b) that the lender and the borrower (or the guarantor) could reasonably be assumed to have the capacity to protect their own interests in the transaction. Corp C §25118(f)-(g). No filings are required to establish either of these exemptions.

© The Regents of the University of California

§16.23 E. Loan Agreement and Promissory Note

The following loan agreement and promissory note forms reflect basic loan transaction terms that might be used in connection with a loan by a founder or nonbank third party associated with the company. A commercial lending institution will require the transaction to be documented on its own form agreements.

© The Regents of the University of California

§16.24 1. Form: Loan Agreement

To download **Word** version, right click and choose *Save Target As*

To download **WordPerfect** version, right click and choose *Save Target As*

LOAN AGREEMENT

THIS LOAN AGREEMENT (the "Loan Agreement") is made and entered into as of _ _[*date*]_ _, by and between _ _[*name of lender*]_ _, a _ _[*lender's entity*]_ _ ("Lender"), and _ _[*name of borrower*]_ _, a California corporation ("Borrower"), with respect to the following:

A. Borrower has requested Lender to make a loan to Borrower to allow Borrower to fund certain of its working capital needs.

B. Lender has agreed to make the loan described in this Loan Agreement on the terms and conditions set forth in this Loan Agreement.

NOW, THEREFORE, in consideration of the covenants and agreements of the parties set forth in this Loan Agreement and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties, intending to be legally bound, agree as follows.

1. DEFINITIONS. Unless a particular word or phrase is otherwise defined or the context requires otherwise, capitalized terms used in this Loan Agreement shall have the meanings set forth below.

1.1. BUSINESS. The term "Business" shall mean the business operations contemplated to be conducted by Borrower in accordance with the Borrower's business plan dated _ _[*date*]_ _.

1.2. BUSINESS DAY. The term "Business Day" shall mean any day on which Lender's office is open for business, other than Saturdays, Sundays, and legal holidays designated by federal law.

1.3. EFFECTIVE DATE. The term "Effective Date" shall mean the date on which Borrower has satisfied the conditions set forth in Section 5.

1.4. EVENT OF DEFAULT. The term "Event of Default" shall have the meaning set forth in Section 6 of the Loan Agreement.

1.5. INDEBTEDNESS. The term "Indebtedness" means (a) indebtedness created, issued, or incurred by Borrower for borrowed money (whether by loan or the issuance and sale of debt securities), whether or not recourse is limited to specific assets of Borrower, including, without limitation, the Promissory Note; (b) obligations of Borrower to pay the deferred purchase or acquisition price of property or services, other than trade accounts payable arising in the ordinary course of business as long as such trade accounts payable are not for borrowed money and are paid within 180 days of the date the respective goods are delivered or the respective services are rendered (unless such trade account payable is being contested in good faith and a sufficient cash reserve, as reasonably determined by Lender, has been established); (c) indebtedness of others secured by a lien on the property of Borrower, whether or not the indebtedness so secured has been assumed by Borrower; (d) obligations of Borrower in respect of letters of credit or similar instruments issued or accepted by banks and other financial institutions for the account of Borrower; and (e) indebtedness of others guaranteed by Borrower.

1.6. LOAN DOCUMENTS. The term "Loan Documents" means all documents executed by Borrower and all documents otherwise executed for the benefit of Lender in connection with the Loan. The term "Loan Documents" includes, but is not limited to, this Loan Agreement, the Promissory Note, the Security Agreement, and any future or additional documents or writings executed under the terms of this Loan Agreement or any amendments or modifications hereto.

1.7. OBLIGATIONS. The term "Obligations" means the Borrower's obligation to pay to Lender (a) any and all sums due Lender under the Loan or otherwise under the terms of the Loan Documents; (b) in the event of any proceeding to enforce the collection of the Obligations, or any of them, after an Event of Default, the reasonable expenses of any exercise by Lender of its rights, together with reasonable attorney fees, expenses of collection, and court costs, as provided in the Loan Documents; and (c) any other indebtedness or liability of Borrower to Lender, whether direct or indirect, absolute or contingent, now or hereafter arising, as provided

in the Loan Documents.

1.8. PRINCIPAL BALANCE. The term "Principal Balance" means the outstanding principal balance under the Loan or the Promissory Note from time to time, as evidenced in Lender's account ledger on which the Principal Balance and all payments relating to the Loan shall be entered, which account ledger will be definitive as to the amounts outstanding.

1.9. PROMISSORY NOTE. The term "Promissory Note" means the promissory note in form and substance as attached as Exhibit A hereto.

1.10. SECURITY AGREEMENT. The term "Security Agreement" means the security agreement in form and substance as attached as Exhibit B hereto.

2. TERMS OF THE LOAN

2.1. NATURE OF FACILITY; USE OF PROCEEDS. Subject to the terms and conditions of the Loan Documents, including all conditions precedent set forth in Section 5, Lender agrees to lend to Borrower and Borrower agrees to borrow from Lender funds in the aggregate principal amount of _ _[*dollar amount*]_ _ Dollars (_ _[*dollar amount*]_ _) (the "Loan"). The duties and obligations of Borrower to repay the Loan shall be evidenced by this Loan Agreement, the Promissory Note, and the Security Agreement. In the event of any conflict in the terms of the Loan Agreement, the Promissory Note, or the Security Agreement, the terms of this Loan Agreement shall govern. The Loan shall be secured as provided in the Security Agreement. Borrower shall apply the proceeds of the Loan to _ _[*describe how funds will be used*]_ _.

Comment: This loan is a secured term loan, the repayment obligations of which are reflected in the corresponding promissory note. See §16.25. Describing the purpose of the loan limits the uses the borrower can make of the funds. For example, a loan may be intended to support acquisition activity, purchase certain identified equipment, or finance specified software development efforts. Alternatively, the loan can be for general operating purposes.

2.2. INTEREST RATE. The Principal Balance of all monies advanced by Lender under the Loan shall bear interest at a rate equal to the lower of (a) of _ _[*number*]_ _% per annum, or (b) the highest rate permitted by applicable law, compounded annually on the basis of a 365-day year, commencing on the date of this Loan Agreement (the "Interest Rate").

Comment: The applicable interest rate may be fixed, as shown here, or may be floating with reference to a base or reference rate, such as the prime rate or the London Interbank Offered Rate, commonly known as LIBOR. If a reference rate is used, the source of the rate should be specified, *e.g.,* "as published in the Wall Street Journal," as well as the frequency of the rate adjustment, *e.g.,* "adjusted quarterly on the first day of each calendar quarter." See §16.22 for discussion of usury issues.

2.3. CALCULATION OF INTEREST. Interest shall accrue on the Loan on the basis of a 360-day year. Borrower agrees that any calculation of amounts accruing hereunder at the Interest Rate shall in each instance be made by Lender and shall, if determined in good faith, be conclusive and binding on Borrower in the absence of manifest error.

2.4. PREPAYMENT. Borrower shall have the right to prepay all or any portion of the Loan outstanding at any time without penalty.

Comment: It is important to specify whether a penalty attaches if a loan is prepaid before its maturity date, particularly if the loan is taken at a high interest rate and could be refinanced later at a lower rate. In loans from noninstitutional sources, prepayment penalties are infrequent.

3. REPRESENTATIONS AND WARRANTIES OF BORROWER. To induce Lender to make the Loan and to enter into the Loan Documents, Borrower makes the following representations and warranties, which shall be true and correct as of the date hereof and throughout the term of this Loan Agreement:

3.1. STATUS OF BORROWER; POWER AND AUTHORITY. Borrower is a corporation duly formed, validly existing, and in good standing under the laws of the State of California. Borrower has the power to borrow and to execute, deliver, and carry out the terms and provisions of the Loan Documents. Borrower has taken or caused to be taken all necessary action to authorize the execution, delivery, and performance of the Loan Documents and the borrowing thereunder.

3.2. NO CONFLICTS OR DEFAULTS. Borrower's entry into this Loan Agreement and the other Loan Documents will not immediately, or with the passage of time, the giving of notice, or both, (a) violate the provisions of the Articles of Incorporation or Bylaws of Borrower; (b) violate any governmental laws or

regulations applicable to Borrower; (c) result in a material default under any material contract, agreement, or instrument to which Borrower is a party; or (d) result in the creation or imposition of any security interest in, or lien, charge, or encumbrance on, any of Borrower's assets.

3.3. LITIGATION. Borrower is not subject to any order of, or written agreement or memorandum of understanding with, any governmental authority. To the best of Borrower's knowledge, there are no actions, suits, claims, investigations, or proceedings pending at law or in equity or before or by any governmental authority, or threatened against Borrower or any of its assets or properties or the transactions contemplated by this Loan Agreement.

3.4. VALIDITY, BINDING NATURE, AND ENFORCEABILITY OF THE LOAN DOCUMENTS. The Loan Documents executed by Borrower constitute the legal, valid, and binding obligations of Borrower and are enforceable against Borrower in accordance with their terms, except as limited by bankruptcy, insolvency, or other laws of general application relating to the enforcement of creditors' rights.

4. BORROWER'S COVENANTS

4.1. AFFIRMATIVE COVENANTS. Borrower covenants and agrees, during the term of the Loan and while any Obligations are outstanding and unpaid, to perform all the acts and promises required by the Loan Documents and all the acts and promises set forth in Sections 4.1(a) through 4.1(d).

(a) PAYMENT AND PERFORMANCE. Borrower shall pay and perform all Obligations in full when and as due under the terms of the Loan Documents (taking into account notice requirements and applicable grace periods), time being strictly of the essence.

(b) MAINTENANCE OF STATUS. Borrower shall take all necessary steps to (1) preserve its existence as a corporation, including, but not limited to, the payment and discharge of all rents, rates, taxes, assessments, and other governmental charges on Borrower or its assets before the date on which interest and penalties attach thereto, and (2) preserve its material franchises and material permits. Borrower shall not materially change, dissolve, or liquidate the corporation, or the nature of its Business or operations during the term of the Loan as such Business and operations exist as of the Effective Date, without the prior written consent of Lender.

(c) FINANCIAL STATEMENTS AND OTHER INFORMATION. During the term of the Loan, Borrower shall furnish to Lender (1) as soon as available, but in any event within 45 days after the close of each quarter, other than the last quarter of the fiscal year of Borrower, commencing with the quarter ending _ _[*date*]_ _, unaudited consolidated balance sheets of Borrower and its subsidiaries as of the end of such quarter, together with the related unaudited consolidated statements of income and retained earnings for such quarter and for the period from the beginning of the fiscal year to the end of such quarter (which shall also set forth any budgeted figures) and cash flows, all in reasonable detail, which balance sheets and statements shall be certified by the President or Chief Financial Officer of Borrower to be accurate to the best of his or her knowledge, subject to year-end adjustments; and (2) as soon as available, but in any event within 90 days after the end of each fiscal year of Borrower, (i) the consolidated balance sheet of the Borrower as at the end of such fiscal year and the related statements of income and changes in the financial position for such fiscal year, in each case setting forth in comparative form the figures for the previous year (if any) of the Borrower, reported on by independent certified public accountants of recognized standing; (ii) any management letters provided by such accountants to the Borrower in connection with their report referred to in (i); and (iii) the consolidated balance sheet of Borrower as at the end of the fiscal year and the related statement of income and changes in financial position for such fiscal year, in each case showing intercompany eliminations, certified by a responsible officer of the Borrower as being fairly stated in all material respects.

Comment: If the loan is from an insider who is a shareholder and also serves on the board, these types of reporting provisions may be waived. Many early-stage companies cannot afford audited financial statements, and care should be taken to make sure that the company can actually comply with any reporting obligations imposed by the loan agreement.

(d) FURTHER ASSURANCES. Borrower agrees to execute such other and further documents as may from time to time in the reasonable opinion of Lender be necessary to perfect, confirm, establish, reestablish, continue, or complete the purposes and intentions of this Loan Agreement.

4.2. NEGATIVE COVENANTS. The Borrower covenants and agrees that, without the Lender's prior written consent, from and after the Effective Date and until all the Obligations are paid in full:

(a) FUNDAMENTAL CHANGES. Borrower shall not, directly or indirectly, by operation of law or otherwise, merge or consolidate with any person, liquidate, wind-up, or dissolve itself (or suffer any liquidation or dissolution), or sell, assign, lease, or otherwise dispose of (whether in one transaction or in a series of

transactions) all or substantially all of its assets (whether now owned or hereafter acquired) to any person; provided that (1) subsidiaries of Borrower may merge with and into Borrower; and (2) subsidiaries of Borrower may merge with and into other subsidiaries of Borrower, provided that the surviving subsidiary assumes the obligations of such nonsurviving subsidiary under this Loan Agreement.

(b) ACQUISITIONS. Borrower shall not acquire any businesses other than corporations or other entities in the same or similar business and Borrower shall be the parent or surviving corporation after giving effect to such acquisition. Notwithstanding the foregoing, Borrower shall not make any acquisition if an Event of Default has occurred and is continuing hereunder at the time of such acquisition.

(c) INDEBTEDNESS. Borrower shall not, directly or indirectly, create or suffer to exist any direct, indirect, fixed, or contingent liability for, or incur, any Indebtedness in excess of _ _[*dollar amount*]_ _ in the aggregate other than (1) current accounts payable arising in the ordinary course of business; (2) other Indebtedness as disclosed to and approved by Lender; (3) the Obligations; (4) deferred taxes; (5) Indebtedness in an aggregate amount not exceeding, at any time, 50% of the capital expenditures approved by Borrower's Board of Directors consisting of either capital leases or Indebtedness secured by purchase money liens covering fixed assets (*i.e.,* property, plant, and equipment); and (6) intercompany loans and advances among the Borrower and its subsidiaries, provided that any Indebtedness of Borrower to any subsidiary shall be subordinated to the Obligations of Borrower to Lender.

(d) LIENS. Borrower shall not create or permit to exist any lien on any of its properties or assets except (1) presently existing or subsequently created liens securing the Obligations; (2) liens granted to secure Indebtedness permitted by Section 4.2(c) hereof; (3) permitted liens and liens listed on Schedule _ _ attached hereto; and (4) purchase money liens covering fixed assets (*i.e.,* property, plant, and equipment) created to secure the payment of Indebtedness permitted by Section 4.2(c); provided, however, that each of such liens shall cover only the fixed assets so acquired and fixed improvements thereon.

(e) RESTRICTED PAYMENT. Borrower shall not (1) declare any cash dividend; (2) incur any other payment or distribution of cash or other property or assets in respect of the capital stock of Borrower other than stock dividends on common stock; or (3) make any payment on account of the purchase, redemption, or other retirement of the capital stock of the Borrower; provided, however, that the foregoing shall not prevent or prohibit Borrower from (i) purchasing shares of the common stock held by its employees, directors, or consultants on termination of their service with or to Borrower, for an amount not in excess of the price specified in the agreements entered into with such employees, directors, and consultants; or (ii) purchasing its own shares after issuance thereof after the Effective Date in an aggregate amount equal to or less than the aggregate net proceeds from the issuance of such shares, provided that Borrower shall be in compliance with all of the covenants set forth in Section 4 hereof.

(f) OTHER AGREEMENTS. Borrower shall not enter into any agreement containing any provision that would be violated or breached by the performance of its obligations under this Loan Agreement or under any of the Loan Documents.

Comment: Negative loan covenants can interfere with the borrower's future business plans. The covenants in Section 4.2 should be reviewed carefully and possibly renegotiated depending on the relationship between the borrower and the lender and the amount of leverage each has in the transaction.

5. REQUIRED DOCUMENTS. As a condition precedent to all duties and obligations of Lender under the Loan Documents, Borrower shall have delivered to Lender the following:

5.1. AUTHORIZATIONS. A certified copy of any consents and authorizations adopted by Borrower and its Board of Directors in a form reasonably acceptable to Lender, authorizing the transactions contemplated by this Loan Agreement and appointing an authorized signatory or signatories to execute all Loan Documents and any other documents connected with the Loan.

5.2. GOVERNING DOCUMENTS. A copy of the Borrower's Articles of Incorporation certified by the Secretary of State of California, with any amendments thereto, and a copy of Borrower's Bylaws, with any amendments thereto, certified by the President or Secretary of Borrower.

5.3. OFFICERS' INCUMBENCY. A certificate of incumbency for the officers of the Borrower.

5.4. EXECUTED LOAN DOCUMENTS. Executed original of the Promissory Note, the Security Agreement, and all other Loan Documents, in form and substance satisfactory to Lender.

5.5. OTHER DOCUMENTS. Such other documents as Lender reasonably may require.

Comment: If a legal opinion is to be required, that should be specified in this section.

6. EVENTS OF DEFAULT. In addition to any occurrences described as an Event of Default in the other Loan Documents, the matters described in Sections 6.1-6.8 shall constitute Events of Default and shall entitle Lender to exercise the rights and remedies under Section 7 and under the other Loan Documents.

6.1. FAILURE TO PAY. Borrower's failure to pay any sum of money owed to Lender in connection with the Obligations, whether principal, interest, penalty, premium, fee, charge, or assessment, as provided in the Loan Documents, on or before the close of business for Lender on the 10th Business Day after the date when due, time being strictly of the essence.

Comment: If a borrower has multiple loan obligations to a single creditor (such as multiple term loans or a term loan and an operating line of credit), it is common for the lender to impose cross-default provisions, under which a default under one obligation constitutes, at the lender's option, a default under the others. A cross-default clause permits the lender to accelerate all loan obligations at once on an event of default and to enforce repayment of the entire outstanding principal balance of all loans.

6.2. FAILURE OF WARRANTY OR REPRESENTATION TO BE TRUE. The failure of any representation or warranty provided by Borrower in the Loan Documents to be materially true.

6.3. FAILURE TO PERFORM AFFIRMATIVE COVENANTS; VIOLATION OF NEGATIVE COVENANTS. Borrower's failure to perform any of the affirmative covenants provided in Section 4.1 or Borrower's violation of any of the negative covenants set forth in Section 4.2.

6.4. DEFAULT UNDER LOAN DOCUMENTS. Borrower's breach of any of the material terms, covenants, or conditions set forth in the Loan Documents. The parties expressly understand and agree that a breach or default by Borrower under any of the Loan Documents and the expiration of all applicable cure periods shall be a breach or default by Borrower under all of the Loan Documents.

6.5. JUDGMENTS. Borrower's suffering uninsured final judgments for payment of money in a material amount (considering Borrower's then current financial condition and the amount of the Principal Balance then outstanding), individually or in the aggregate, and Borrower's failure to discharge the same within a period of 60 days, unless execution has been effectively stayed, whether by appeal, the posting of a bond, or otherwise.

6.6. BORROWER'S INVOLUNTARY BANKRUPTCY. Entry of a decree or order for relief, by a court having jurisdiction, against or with respect to Borrower in an involuntary case (or the failure of any such case to be dismissed within ninety (90) days of its commencement) under federal bankruptcy laws or any state insolvency or similar laws requiring (a) the liquidation of Borrower; (b) a reorganization of Borrower or the Business; or (c) the appointment of a receiver, liquidator, assignee, custodian, trustee, or similar official for Borrower or any of the properties of Borrower.

6.7. BORROWER'S VOLUNTARY BANKRUPTCY. Borrower's (a) commencement of a voluntary case under federal bankruptcy laws or any state insolvency or similar laws; (b) consent to the appointment for taking possession by a receiver, liquidator, assignee, custodian, trustee, or similar official for Borrower of any of its property; (c) making any assignment for the benefit of creditors; or (d) failing generally to pay its debts as they become due, either as to the amount of such debts or the number of such debts.

6.8. DISSOLUTION. Borrower's commencement or becoming the subject of any dissolution proceedings; undertaking any action for the purpose of dissolving and winding up Borrower; or resolving to take or taking any action for the purpose of surrendering any right, license, franchise, or other incident of Borrower's existence.

7. REMEDIES

7.1. LENDER'S SPECIFIC RIGHTS AND REMEDIES. On the happening of any Event of Default, subject to the provisions of Section 7.4, Lender, in addition to any and all rights provided by law or equity, may:

(a) Accelerate and call due the unpaid Principal Balance of the Loan, and all accrued interest and other sums due thereunder;

(b) File suit against Borrower or any other party to any of the Loan Documents; and

(c) Exercise all other rights and remedies provided by this Loan Agreement or the other Loan Documents.

7.2. COLLECTION COSTS. If suit or action is instituted to enforce any of the terms of this Loan Agreement or of any other Loan Documents, the prevailing party shall be entitled to recover from the other party its attorney fees and costs in addition to all other sums provided by law.

7.3. NOTICE OF DEFAULT. Lender shall provide Borrower with (a) 10 Business Days' prior written notice and an opportunity to cure any default arising from Borrower's failure to satisfy a payment obligation under the Loan Documents, and (b) 30 Business Days' prior written notice and an opportunity to cure any other act or omission constituting an Event of Default under the Loan Documents. Notwithstanding anything to the contrary stated herein, Borrower shall not be entitled to any notice or opportunity to cure any of the Events of Default described in Sections 6.6, 6.7 and 6.8.

8. RIGHT OF FIRST REFUSAL. During the 5 years following the Effective Date, if Borrower decides that it requires additional debt financing _ _[*to fund _ _[describe purpose, e.g., the acquisition of XYZ Company*]_ _]_ _, then Borrower shall provide Lender with written notice (the "Offer Notice") of such debt financing requirements. Lender shall have 10 Business Days from the date of the Offer Notice to accept or reject the Offer Notice (the "Offer Period"). If Lender fails to accept or reject the Offer Notice in writing within the Offer Period, then Lender shall be deemed to have waived its right to provide such additional debt financing to Borrower. If Lender advises Borrower in writing that it desires to provide such debt financing, then Lender shall fund such debt financing within 10 Business Days following the written acceptance by Lender of the Offer Notice, on Borrower's delivery to Lender of (a) such loan documentation as a bona fide third party was prepared to accept from Borrower; or (b) loan documentation substantially similar to the Loan Documents (except for changes necessary to make such documents reflect the financial terms as set forth in the Offer Notice), together with a copy of Borrower's projections and analyses, with respect to such _ _[*e.g., potential acquisition targets*]_ _.

Comment: This provision is intended to require the borrower to provide the lender an opportunity to meet any further debt financing requirements of the borrower before the borrower seeks financing from a third party. The type of additional debt financing that will trigger this provision should be limited, *e.g.* (as here) to the funding of a particular type of project or operational activity, or by a minimum dollar amount, so that the company may obtain credit cards, equipment leases, and small loan amounts without having to seek a waiver from the lender.

9. GENERAL PROVISIONS

9.1. MODIFICATIONS. The Loan Documents may be amended, changed, or modified only as may be agreed in writing by Borrower and Lender from time to time.

9.2. BINDING EFFECT. The Loan Documents shall be binding on the parties and their successors and assigns. The rights and benefits of any party under the Loan Documents may not be assigned without the prior written consent of the other party, which consent may be granted or withheld in such other party's sole and absolute discretion.

9.3. ENTIRE AGREEMENT. The Loan Documents embody the entire agreement of the parties relating to the Loan. There are no promises, terms, conditions, obligations, or warranties other than those contained in the Loan Documents. The Loan Documents supersede all prior communications, representations, or agreements, verbal or written, between the parties relating to the Loan.

9.4. GOVERNING LAW. The validity, meaning, enforceability, and effect of the Loan Documents and the rights and liabilities of the parties shall be determined in accordance with the laws of the State of California. All parties acknowledge and hereby stipulate for the purpose of any future proceedings that the Loan Documents and all subsequent writings or documents relating or pertaining thereto are to be considered for all purposes, including, but not limited to, choice of law determinations, to have been executed and delivered by all parties within the actual geographic boundaries of California, even if such loan documents were, in fact, executed and delivered elsewhere.

9.5. INCORPORATION BY REFERENCE. All documents, instruments, attachments, exhibits, and other writings executed with, referred to in, or attached to this Loan Agreement are incorporated by reference into this Loan Agreement and are made a part of this Loan Agreement as if fully set out herein. This Loan Agreement, before such incorporation, controls in the event of any conflict with the terms of the Loan Documents.

9.6. JURISDICTION AND VENUE. BORROWER CONSENTS TO THE VENUE AND JURISDICTION OF ANY COURT, STATE OR FEDERAL, LOCATED IN THE COUNTY OF _ _[*COUNTY NAME*]_ _. BORROWER AGREES THAT ANY ACTION, PROCEEDING, OR OTHER MATTER ARISING DIRECTLY OR INDIRECTLY UNDER THIS LOAN AGREEMENT MAY BE BROUGHT BY LENDER IN ITS SOLE DISCRETION IN ANY SUCH COURT. BORROWER AGREES TO THAT VENUE FOR ANY ACTION, PROCEEDING, OR OTHER MATTER PROPERLY PLACED IN ANY SUCH COURT LOCATED IN THE COUNTY OF _ _[*COUNTY NAME*]_ _. Borrower consents and agrees that any service of process may be made on Borrower wherever Borrower can be located or by certified mail directed to Borrower at Borrower's address set forth in Section 9.7 (with a copy to Borrower's counsel at the most recent notice address). This provision is permissive, not mandatory, and Lender reserves the right to

bring any action, proceeding, or other matter arising directly or indirectly under this Loan Agreement against Borrower wherever either the Borrower or its properties might be found or might otherwise be subject to jurisdiction.

9.7. NOTICES. Any notice under the Loan Documents shall be in writing, without implying the obligation to provide such notice. Any notice to be given or document to be delivered under the Loan Documents shall be deemed to have been duly received on (a) delivery, if delivered in person or by any expedited delivery service that provides proof of delivery; (b) tested telex; or (c) the 5th Business Day after mailing, if mailed by certified mail, return receipt requested, postage prepaid, addressed to Lender or Borrower at the appropriate addresses. The addresses for notices are those set forth below or such other addresses as may be hereafter specified by written notice by the parties:

If to Lender: _ _[*Lender's name and address*]_ _

If to Borrower: _ _[*Borrower's name and address*]_ _

9.8. RELATIONSHIP OF THE PARTIES. Neither Lender nor Borrower shall be deemed a partner, joint venturer, agent, or related entity of the other by reason of the Loan Documents.

9.9. SEVERABILITY. If a court of competent jurisdiction finds any term or provision of this Loan Agreement, or the application thereof to any person or circumstance, to be invalid, void, or unenforceable to any extent, (a) such court may amend and/or interpret such term or provision so that it will be valid to the fullest extent possible under law; and (b) the remaining provisions of this Loan Agreement and any application thereof shall continue in full force and effect without being impaired or invalidated in any way.

9.10. TIME. Time is of the essence under this Loan Agreement.

9.11. USURY. Borrower and Lender intend to comply with applicable usury laws. Accordingly, notwithstanding any provision in this Loan Agreement or in any other Loan Document to the contrary, neither this Loan Agreement nor any other Loan Document shall require the payment, or permit the collection, of interest in excess of the maximum amount permitted by law. If compliance with this Loan Agreement or any other Loan Document would result in a violation of applicable usury law, the amount of the payment obligation imposed by this Loan Agreement or any other Loan Document shall be reduced to the maximum amount permitted by law.

9.12. WAIVERS. Lender may at any time or from time to time waive all or any rights under any of the Loan Documents, but any waiver or indulgence at any time or from time to time shall not constitute, unless specifically so expressed by Lender in writing, a future waiver by Lender of performance by Borrower.

9.13. COUNTERPARTS. This Loan Agreement may be executed in multiple counterparts, all of which together shall constitute one instrument.

IN WITNESS WHEREOF, Borrower and Lender have executed this Loan Agreement as of the date first written above.

Date: _ _ _ _ _ _

_ _[*NAME OF LENDER*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

Date: _ _ _ _ _ _

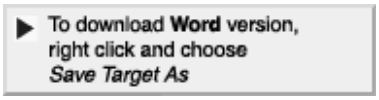
_ _[*NAME OF BORROWER*]_ _,
a _ _[*state of incorporation*]_ _ **corporation**

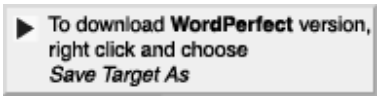
By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/16 Financing an Online Business/§16.25 2. Form: Promissory Note

§16.25 2. Form: Promissory Note





PROMISSORY NOTE

_ _[*Dollar amount*]_ _
_ _[*Date*]_ _
_ _[*City*]_ _**, California**

FOR VALUE RECEIVED, the undersigned, _ _[*Borrower's name*]_ _, a California corporation ("Borrower"), promises to pay to the order of _ _[*Lender's name*]_ _ ("Holder") at _ _[*Lender's address*]_ _, or such other address as Holder may notify Borrower, the principal sum of _ _[*dollar amount*]_ _, together with interest as provided herein. This Note is made pursuant to and is subject to the terms and conditions of that certain Loan Agreement of even date herewith, between Holder and Borrower (as amended or modified from time to time, the "Loan Agreement"). This Note is secured pursuant to the terms of a Security Agreement of even date herewith between Borrower and Holder. Capitalized terms not otherwise defined herein have the meanings set forth in the Loan Agreement.

The principal amount due hereunder shall be paid to Holder as follows:

_ _[*Dollar amount*]_ _ **on** _ _[*date*]_ _**,**

_ _[*Dollar amount*]_ _ **on** _ _[*date*]_ _**, and**

_ _[*Dollar amount*]_ _ **on** _ _[*date*]_ _**.**

Comment: Under this loan, principal payments are made in fixed periodic installments. Principal payments may be made on a periodic basis (*e.g.,* monthly, quarterly, or annually), on fixed dates, or in a lump sum at the end of the term. The term of the loan can be fixed, as here, with payment due on a specific date or payable "on demand," meaning that the lender can call for the payment of the note on written notice, at which time the full amount is due.

Interest on the unpaid principal balance shall accrue from the date hereof and shall be computed on the basis of a 360-day year, for the actual number of days elapsed, on the outstanding unpaid principal amount hereunder, at a per annum rate equal to the lower of (1) _ _[*number*]_ _% per annum, or (2) the highest rate permitted by applicable law, compounded annually on the basis of a 365-day year, commencing on the date hereof. On the 1st day of each month following the end of the 6th calendar month following the date of this Note, Borrower shall pay Holder accrued interest in arrears. For the 6 calendar months following the date of this Note, interest shall accrue at the aforementioned rate, and such accrued interest shall be payable on _ _[*date*]_ _.

Comment: Under this form of promissory note, interest and principal are paid at different intervals to illustrate how flexible payment structures can be. Consider structuring payments to match the company's projected cash flow. Here, principal is paid on fixed dates and interest is deferred for the first six months of the loan and payable monthly thereafter. Also consider how interest rates may be set to meet cash flow needs while accommodating the lender. Rates can be set higher in early periods (to provide an incentive to the lender to make the loan), then decrease as the debtor shows the ability to pay on time.

All payments of principal and interest on this Note shall be made to Holder in United States dollars, in immediately available funds. Principal and interest hereunder may be prepaid in part or in full at any time without penalty. Any prepayment of this Note will be credited first against accrued and unpaid interest, then principal. On payment in full of the amount of all principal and interest payable hereunder, this Note shall be surrendered to the Borrower for cancellation.

In addition to all remedies provided by law, on an Event of Default, Holder may, at its option:

(a) Declare this Note immediately due and payable; and

(b) Exercise any and all remedies provided for in the Loan Agreement and the Security Agreement.

If this Note is submitted to an attorney for collection, or suit is brought on this Note, or this Note is collected through bankruptcy or other judicial or alternative dispute resolution proceedings, Borrower agrees and promises to pay reasonable attorney fees and all collection costs and out-of-pocket expenses incurred by Holder.

This Note has been executed and delivered in, and shall be governed by and construed in accordance with the laws of, the State of California. Borrower hereby irrevocably submits to the jurisdiction of any state or any federal court sitting in _ _[*name*]_ _ County, California, in any action or proceeding brought to enforce, or otherwise arising out of or relating to, this Note and hereby waives any objection to venue in any such court and any claim that such forum is an inconvenient forum.

Borrower waives presentment for payment, protest, and notice of protest for nonpayment of this Note and waives trial by jury in any action under or relating to this Note. Any notice, other communication, or payment required or permitted hereunder shall be in writing and shall be deemed to have been given on delivery to the address provided in the Loan Agreement.

Date: _ _ _ _ _ _

_ _[*NAME OF BORROWER*]_ _,
a _ _[*state of incorporation*]_ _ **corporation**

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

PRACTICE TIP: Most promissory notes are negotiable instruments under Division 3 of the California Commercial Code, and each original signed note represents a separate obligation to pay. Thus, only one original should be signed, and the lender should retain the original in a safe location. When the debt has been paid in full, the note should be destroyed or marked "paid in full."

© The Regents of the University of California

F. Security Interests in Intellectual Property Collateral

§16.26 1. Generally

Because a substantial part of the valuable assets of Internet-based businesses may consist of intellectual property, an understanding of the issues in perfecting security interests in intellectual property is important for both e-business borrowers and their lenders. Sections 16.27-16.31 provide an overview of the methods for perfecting security interests in different types of intellectual property collateral. A model form of security agreement covering intellectual property is in §§16.32-16.33.

Security interests in most types of personal property are governed by Article 9 of the Uniform Commercial Code (UCC) as enacted in each state. See Com C §§9101-9709. Intellectual property is intangible personal property, classified as a "general intangible" under the UCC. Com C §9102(a)(42). In general, for a lender to obtain an enforceable security interest in most types of collateral (including intellectual property), value must be given, the borrower must have rights in the collateral, and the borrower must execute a security agreement describing the collateral. Com C §9203(b). In addition, for the lender to be able to enforce its rights in the collateral against transferees of the borrower or a bankruptcy trustee, the security interest must be perfected. See Com C §§9317, 9322. Security interests in most types of personal property collateral can be perfected by filing a UCC-1 financing statement with the office of the applicable Secretary of State. Com C §§9310, 9501. If the borrower is a corporation, a limited liability company, or a limited partnership, the applicable state for filing is the state in which the borrower was organized, *e.g.,* Delaware for Delaware corporations, California for California corporations. Com C §9307. Security interests in intellectual property, however, may or may not be perfected by filing a UCC-1 financing statement, depending on the extent to which federal law preempts the UCC for the particular type of intellectual property involved. See Com C §9109(c)(1).

For a comprehensive discussion of security interests in personal property under Division 9 of the California Commercial Code and other applicable law, see Secured Transactions in California Commercial Law Practice (2d ed Cal CEB 2001).

© The Regents of the University of California

§16.27 2. Security Interests in Copyrights

The first reported case to address perfection requirements for security interests in copyrights was *National Peregrine Inc. v Capitol Federal Sav. & Loan Ass'n (In re Peregrine Entertainment Ltd.)* (CD Cal 1990) 116 BR 194. Peregrine held that the proper method for perfection of a security interest in a copyright (and any accounts receivable generated by the copyright) is to file a copy of the security agreement in the U.S. Copyright Office, rather than filing a UCC-1 financing statement with the Secretary of State. See also *Official Unsecured Creditors' Comm. v Zenith Prods., Inc. (In re AEG Acquisition Corp.)* (BAP 9th Cir 1993) 161 BR 50 and *In re Avalon Software, Inc.* (Bankr D Ariz 1997) 209 BR 517 (both of which were overruled by *Aerocon Eng'g, Inc. v Silicon Valley Bank (In re World Auxiliary Power Co.)* (9th Cir 2002) 303 F3d 1120, discussed below). The *Peregrine* court noted that the Copyright Act requires a "transfer" of a copyright to be recorded in the Copyright Office in order to have priority over a later transfer of the same work (17 USC §205) and that "transfer" is defined to include a mortgage or other hypothecation (17 USC §101), which includes a security interest. *Peregrine*, 116 BR at 199. The court held that the Copyright Act preempts the UCC, and that a UCC-1 financing statement is ineffective to perfect a security interest in a copyright.

Peregrine, however, did not distinguish between registered copyrights and unregistered copyrights. In *Aerocon Eng'g, Inc. v Silicon Valley Bank (In re World Auxiliary Power Co.)* (9th Cir 2002) 303 F3d 1120, the Ninth Circuit Court of Appeals held that a Copyright Office filing is not necessary to perfect security interests in unregistered copyrights. The court reasoned that because unregistered works are not searchable in the Copyright Office, recording a security agreement for an unregistered copyright in the Copyright Office could not give constructive notice to subsequent transferees under 17 USC §205(c) and therefore could not preserve the priority of a creditor's security interest. 303 F3d at 1126. Accordingly, filing a UCC-1 financing statement at the state level is sufficient to perfect a security interest in an unregistered copyright. In so holding, the Ninth Circuit expressly adopted the *Peregrine* holding as applied to registered copyrights, but rejected it as applied to unregistered copyrights. The Ninth Circuit also expressly rejected the holdings in *Official Unsecured Creditors' Comm. v Zenith Prods., Inc., supra,* and *In re Avalon Software, Inc., supra,* as applied to unregistered copyrights.

PRACTICE TIP: Despite the *Peregrine* and *Aerocon* holdings, it is standard practice for lenders' counsel perfecting security interests in registered copyrights to file UCC-1 financing statements at the state level as a precaution, as well as filing copies of security agreements with the Copyright Office. Dual filings may be necessary in any event if the security agreement covers other collateral, such as tangible goods for which a UCC-1 financing statement must be filed. When filing a copy of the security agreement with the Copyright Office, the same form of cover sheet as is used for assignments of copyrights must be attached. A sample of the cover sheet is reproduced in §1.11. For unregistered copyrights, the lender will likely require the borrower to prepare and file an application for registration of the copyright so that the lender can make a Copyright Office filing of the security agreement. The Copyright Office may take months to process the application for registration, however. Further, registration will only cover the work described on the application, so subsequent upgrades and improvements will require separate new applications for registration (and refiling of copies of the security agreement) to enable to lender to maintain its security interest on the most current version of the copyrighted work. Finally, registration necessarily involves public disclosure of the work. The borrower may be unwilling to disclose proprietary and confidential works that are critical to its business.

© The Regents of the University of California

§16.28 3. Security Interests in Patents

The law concerning perfection of security interests in patents is well settled. *Moldo v Matsco, Inc. (In re Cybernetic Servs., Inc.)* (9th Cir 2001) 252 F3d 1039, cert denied (2002) 534 US 1130, is the most recent case holding that, to perfect a security interest in a patent, the lender must file a UCC-1 financing statement under applicable state law, but does not need to record its security agreement or a patent assignment in the U.S. Patent and Trademark Office (PTO). The Ninth Circuit in *Cybernetic Servs.* held that nothing in the Patent Act addressed grants of security interests, and therefore the Patent Act did not preempt the UCC. The terms "assignment, grant or conveyance" in §261 of the Patent Act (35 USC §261) cover transfers of ownership interests in a patent only. Therefore, no filings in the PTO are required to perfect a security interest in a patent.

PRACTICE TIP: Although not required for perfection, lenders are nonetheless advised to file a copy of the security agreement with the PTO, in an effort to give actual notice of their security interest to any potential transferee of an ownership interest in the patent. See *Moldo v Matsco, Inc. (In re Cybernetic Servs., Inc.)* (BAP 9th Cir 1999) 239 BR 917, 921 n10, aff'd (9th Cir 2001) 252 F3d 1039, cert denied (2002) 534 US 1130 (recording of security interest is discretionary with PTO, therefore serves to provide actual notice, rather than constructive notice, to bona fide purchasers of patents); *In re Transportation Design & Technol., Inc.* (Bankr SD Cal 1985) 48 BR 635, 640 (secured creditor must record security agreement with PTO to prevent borrower from transferring title to patent free and clear of security interest before debt is repaid). If recording a copy of the security agreement in the PTO, the same form of cover sheet as is used for assignments of patents must be attached. A sample of the cover sheet is reproduced in §2.17.

© The Regents of the University of California

§16.29 4. Security Interests in Trademarks

Courts have uniformly held that the Lanham Act (15 USC §§1051-1141n), like the Patent Act, does not preempt the UCC, and that to perfect a security interest in a trademark, only a UCC-1 financing statement need be filed in the applicable state office. No filing in the U.S. Patent and Trademark Office (PTO) is required. *In re Together Dev. Corp*. (Bankr D Mass 1998) 227 BR 439, 441, aff'd (D Mass 2000) 255 BR 606; *Joseph v 1200 Valencia, Inc. (In re 199Z, Inc.)* (Bankr CD Cal 1992) 137 BR 778, 782; *In re Roman Cleanser Co*. (Bankr ED Mich 1984) 43 BR 940, 944, aff'd (6th Cir 1986) 802 F2d 207. As in the case of patents, however (see Practice Tip in §16.28), filing a copy of the security agreement in the PTO is nevertheless advisable in an effort to give actual notice to subsequent transferees of the trademark. If a copy of the security agreement is to be filed in the PTO, the same form of cover sheet as is used for assignments of trademarks must be attached. A sample of the cover sheet is reproduced in §3.59. If the trademark has been registered under state law, either in place of or in addition to federal registration, filing a copy of the security agreement in state trademark records is also advisable. See Bus & P C §14220.

As discussed in §3.57, any assignment of a trademark that is not accompanied by an assignment of the goodwill of the business associated with use of the trademark (an assignment "in gross") is invalid. See 15 USC §1060; *E. & J. Gallo Winery v Gallo Cattle Co.* (9th Cir 1992) 967 F2d 1280. For this reason, a trademark security interest should not be documented by using a collateral assignment, but rather with a conventional form of security agreement, such as the one set forth in §16.33. In *Clorox Co. v Chemical Bank* (TTAB 1996) 40 USPQ2d 1098, the Trademark Trial and Appeal Board cancelled the trademark registration for a mark that had been assigned to Chemical Bank as loan collateral in violation of the Lanham Act's prohibition on assignments of intent-to-use applications. See 15 USC §1060. See also *In re Roman Cleanser Co*. (6th Cir 1986) 802 F2d 207 (trademark security interest was not invalid assignment "in gross" because it did not cover equipment and machinery necessary to produce trademarked goods).

© The Regents of the University of California

§16.30 5. Security Interests in Domain Names

As discussed generally in chap 3, domain names function as electronic addresses for particular locations on the Internet. They are not necessarily entitled to protection as trademarks or trade names unless they are used by the holder in commerce and qualify under the Lanham Act or applicable state law as such. See generally §§3.23-3.26. They are issued by domain name registrars authorized by the Internet Corporation for Assignment of Names and Numbers (ICANN) pursuant to service agreements.

There are apparently no reported cases to date addressing security interests in domain names. In *Network Solutions Inc. v Umbro Int'l Inc.* (Va 2000) 529 SE2d 80, the Supreme Court of Virginia found that rights in a domain name do not exist separate and apart from the services provided by the registrar that make the domain name operational on the Internet. Thus, a domain name is "a product of a contract for services between the registrar and the registrant." 529 SE2d at 86. The court held that, because the domain name at issue was based on an executory contract, it was not subject to garnishment under the Virginia garnishment statutes.

The *Network Solutions* case indicates that, for purposes of perfection of security interests, lenders should treat domain names as contract rights, *i.e.,* as general intangibles under the UCC (see Com C §9102(a)(42)), and file a UCC-1 financing statement under applicable state law. In addition, if the domain name also serves as a trademark or trade name for a business, the procedures for perfection of security interests in trademarks discussed in §16.29 should be followed. Domain names that are protectible as trademarks or trade names will be subject to the same restrictions against assignments in gross set forth in 15 USC §1060.

© The Regents of the University of California

§16.31 6. Security Interests in Trade Secrets

Trade secrets are protected by state law, and are classified as "general intangibles" under the UCC. See Com C §9102(a)(42). Because there are no federal laws governing trade secrets, the UCC requirements for perfection of security interests are not preempted. To perfect a security interest in a trade secret, a lender must file a UCC-1 financing statement with the applicable state office. See Com C §9310(a). It is important to note that the security agreement and financing statement should not jeopardize confidentiality by actually describing the trade secret. Further, to the extent that a trade secret has been expressed in writing or, *e.g.,* embodied in software code, it may be copyrightable. Therefore, a lender should also consider whether the requirements discussed in §16.27 concerning perfection of security interests in copyrights may be applicable. For further discussion of security interests in trade secrets, see Trade Secrets Practice in California, chap 9 (2d ed Cal CEB 1996).

© The Regents of the University of California

7. Form of Security Agreement (Intellectual Property)

§16.32 a. Introduction

In §16.33 is a model security agreement for intellectual property collateral. For a model form of security agreement covering other types of collateral, see Secured Transactions in California Commercial Law Practice, chap 2 (2d ed Cal CEB 2001).

© The Regents of the University of California

§16.33 b. Form: Security Agreement (Intellectual Property)

To download **Word** version, right click and choose *Save Target As*

To download **WordPerfect** version, right click and choose *Save Target As*

SECURITY AGREEMENT (INTELLECTUAL PROPERTY)

THIS SECURITY AGREEMENT (this "Agreement"), dated as of _ _[*date*]_ _, is made and entered into by and between _ _[*Debtor's name*]_ _, a _ _[*specify entity, e.g., California corporation*]_ _ ("Debtor"), and _ _[*Secured Party's name*]_ _, a _ _[*specify entity, e.g., California corporation*]_ _ ("Secured Party").

Debtor and Secured Party hereby agree as follows:

1. DEFINITIONS AND INTERPRETATION. All capitalized terms used in this Agreement and not otherwise defined herein shall have the meanings assigned to them in the Credit Agreement. As used in this Agreement, the following terms shall have the following meanings:

1.1. "Collateral" has the meaning set forth in Section 2.

1.2. "Copyright Office" means the United States Copyright Office.

1.3. "Credit Agreement" means that certain Credit Agreement, dated as of the date hereof, between Debtor and Secured Party.

[*If patents or trademarks are involved, add*]

1.4. "PTO" means the United States Patent and Trademark Office.

[*Continue*]

1.5. "UCC" means the Uniform Commercial Code as in effect in the State of _ _[*e.g., California*]_ _.

Where applicable in the context of this Agreement and except as otherwise defined herein, terms used in this Agreement shall have the meanings assigned to them in the UCC.

2. SECURITY INTEREST

2.1. GRANT OF SECURITY INTEREST. As security for the payment and performance of the Obligations, Debtor hereby assigns, transfers, and conveys to the Secured Party, and grants a security interest in and mortgage to the Secured Party of, all of Debtor's right, title, and interest in and to the following property, in each case whether now or hereafter existing or arising or in which Debtor now has or hereafter owns, acquires, or develops an interest and wherever located (collectively, the "Collateral"):

(a) COPYRIGHTS. All of Debtor's present and future United States registered copyrights and copyright registrations, including Debtor's United States registered copyrights and copyright registrations listed in Schedule A attached to this Agreement; all of Debtor's present and future United States applications for copyright registrations, including Debtor's United States applications for copyright registrations listed in Schedule A attached to this Agreement; all of Debtor's present and future copyrights that are not registered in the Copyright Office (collectively, the "Copyrights"); and any and all royalties, payments, and other amounts payable to Debtor in connection with the Copyrights, together with all renewals and extensions of the Copyrights, the right to recover for all past, present, and future infringements of the Copyrights, and all manuscripts, documents, writings, tapes, disks, storage media, computer programs, computer databases, computer program flow diagrams, source codes, object codes, and all tangible property embodying or incorporating the Copyrights, and all other rights of every kind whatsoever accruing under or pertaining to the Copyrights;

[*If the collateral includes trademarks, add the next two provisions*]

[(b)] TRADEMARKS. All state (including common law), federal, and foreign trademarks, service marks, and trade names, and all applications for registration of such trademarks, service marks, and trade names (but excluding each application to register any trademark, service mark, or other mark before the filing under applicable law of a verified statement of use [or the equivalent] for such mark) (collectively, the "Marks"); all

licenses relating to any of the Marks and all income and royalties with respect to any licenses (including such marks, names, and applications as described in Schedule A attached to this Agreement), whether registered or unregistered and wherever registered; all rights to sue for past, present, or future infringement or unconsented use of any of the Marks; all rights arising from and pertaining to the Marks; and all reissues, extensions, and renewals of the Marks;

[(c)] GOODWILL. The entire goodwill of or associated with the businesses now or hereafter conducted by Debtor connected with and symbolized by any of the aforementioned properties and assets;

[*If the collateral includes patents, add*]

[(d)] PATENTS. All patents and patent applications, whether domestic or foreign (collectively, the "Patents"); all licenses relating to any of the Patents and all income and royalties with respect to any licenses (including such patents and patent applications as described in Schedule A attached to this Agreement); all rights to sue for past, present, or future infringement of the Patents; all rights arising from and pertaining to the Patents; and all reissues, divisions, continuations, renewals, extensions, and continuations-in-part of the Patents;

[*Continue*]

[(e)] INTANGIBLES. All general intangibles and all intangible intellectual or other similar property of Debtor of any kind or nature associated with or arising out of any of the aforementioned properties and assets and not otherwise described above;

[(f)] LICENSE AGREEMENTS. All of Debtor's right, title, and interest in and to any and all present and future license agreements with respect to the Copyrights _ _[*, Trademarks, and Patents*]_ _;

[(g)] RIGHTS TO PAYMENT. All present and future accounts and other rights to payment arising from, in connection with, or relating to the Copyrights _ _[*, Trademarks, and Patents*]_ _; and

[(h)] PROCEEDS. All cash and noncash proceeds of any and all of the foregoing Collateral (including license royalties, rights to payment, accounts, and proceeds of infringement suits) and, to the extent not otherwise included, all payments under insurance (whether or not Secured Party is the loss payee thereof) or any indemnity, warranty, or guaranty payable by reason of loss or damage to or otherwise with respect to the foregoing Collateral.

2.2. CONTINUING SECURITY INTEREST. Debtor agrees that this Agreement shall create a continuing security interest in the Collateral that shall remain in effect until terminated in accordance with Section 11.

2.3. SUPPLEMENT TO CREDIT AGREEMENT. This Agreement has been granted in conjunction with the security interests granted to Secured Party under the Credit Agreement or other security documents referred to therein. The rights and remedies of Secured Party with respect to the security interests granted herein are without prejudice, and are in addition, to those set forth in the Credit Agreement or any other security documents referred to therein, all terms and provisions of which are incorporated herein by reference.

3. REPRESENTATIONS AND WARRANTIES. Debtor represents and warrants to Secured Party that:

3.1. COPYRIGHT REGISTRATIONS. A true and correct list of all of Debtor's United States registered copyrights and copyright registrations is set forth in Schedule A.

3.2. APPLICATIONS FOR COPYRIGHT REGISTRATION. A true and correct list of all of Debtor's United States applications for copyright registrations is set forth in Schedule A.

[*If Collateral includes trademarks, add*]

3.3. TRADEMARK REGISTRATIONS AND APPLICATIONS. A true and correct list of all of the existing Collateral consisting of United States trademarks, trademark registrations, or applications for trademark registrations owned by Debtor, in whole or in part, is set forth in Schedule A.

[*Continue*]

4. FURTHER ACTS. On a continuing basis, Debtor shall make, execute, acknowledge, and deliver, and file and record in the proper filing and recording places, all such instruments and documents, and take all such action, as may be necessary or advisable or may be requested by Secured Party to carry out the intent and purposes of this Agreement, or for assuring, confirming, or protecting the grant or perfection of the security interest granted or purported to be granted under this Agreement, to ensure Debtor's compliance with this Agreement or to enable Secured Party to exercise and enforce its rights and remedies hereunder with respect to the Collateral, including any documents for filing with the Copyright Office

[*If the Collateral includes trademarks or patents, add*]

or the PTO

[*Continue*]

or any applicable state office. Secured Party may record this Agreement, an abstract thereof, or any other document describing Secured Party's interest in the Collateral with the Copyright Office,

[*If the Collateral includes trademarks or patents, add*]

and with the PTO,

[*Continue*]

at the expense of Debtor. In addition, Debtor authorizes Secured Party to file financing statements describing the Collateral in any UCC filing office deemed appropriate by Secured Party.

5. AUTHORIZATION TO SUPPLEMENT. Debtor shall give Secured Party prompt notice of any additional United States copyright _ _[*trademark or patent*]**_ _ registrations or applications for such registrations _ _**[*and any reissue, division, or continuation of any patent*]**_ _ after the date hereof. Debtor authorizes Secured Party unilaterally to modify this Agreement by amending Schedule A to include any future United States registered copyrights _ _**[*trademarks or patents*]**_ _ or applications therefor of Debtor. Notwithstanding the foregoing, no failure to so modify this Agreement or amend Schedule A shall in any way affect, invalidate, or detract from Secured Party's continuing security interest in all Collateral, whether or not listed on Schedule A.**

6. BINDING EFFECT. This Agreement shall be binding on, inure to the benefit of, and be enforceable by Debtor, Secured Party, and their respective successors and assigns. Debtor may not assign, transfer, hypothecate, or otherwise convey its rights, benefits, obligations, or duties under this Agreement except as specifically permitted by the Credit Agreement.

7. GOVERNING LAW. This Agreement shall be governed by, and construed in accordance with, the laws of the State of _ _[*e.g., California*]**_ _, except as required by mandatory provisions of law or to the extent the perfection or priority of the security interests hereunder, or the remedies hereunder, in respect of any Collateral are governed by the law of a jurisdiction other than _ _**[*same state as specified above*]**_ _.**

8. ENTIRE AGREEMENT; AMENDMENT. This Agreement and the Credit Agreement, together with the Schedules attached to those Agreements, contains the entire agreement of the parties with respect to the subject matter hereof and supersedes all prior drafts and communications relating to such subject matter. Neither this Agreement nor any provision hereof may be modified, amended, or waived except by the written agreement of the parties, as provided in the Credit Agreement. Notwithstanding the foregoing, Secured Party unilaterally may re-execute this Agreement or modify, amend, or supplement the Schedules hereto as provided in Section 5 hereof. To the extent that any provision of this Agreement conflicts with any provision of the Credit Agreement, the provision giving Secured Party greater rights or remedies shall govern, it being understood that the purpose of this Agreement is to add to, and not detract from, the rights granted to Secured Party under the Credit Agreement.

9. COUNTERPARTS. This Agreement may be executed in any number of counterparts and by different parties hereto in separate counterparts, each of which when so executed shall be deemed to be an original and all of which taken together shall constitute one and the same agreement. Delivery of an executed counterpart of this Agreement by facsimile shall be equally as effective as delivery of a manually executed counterpart. Any party hereto delivering a counterpart of this Agreement by facsimile shall also deliver a manually executed counterpart, but the failure to so deliver a manually executed counterpart shall not affect the validity, enforceability, or binding effect hereof.

10. TERMINATION. On payment and performance in full of all Obligations, the security interests created by this Agreement shall terminate, and Secured Party (at Debtor's expense) shall promptly execute and deliver to Debtor such documents and instruments reasonably requested by Debtor as shall be necessary to evidence termination of all such security interests given by Debtor to Secured Party hereunder, including cancellation of this Agreement by written notice from Secured Party to the Copyright Office

[*If the Collateral includes trademarks or patents, add*]

and to the PTO.

[*Continue*]

11. NO INCONSISTENT REQUIREMENTS. Debtor acknowledges that this Agreement and the other documents, agreements, and instruments entered into or executed in connection herewith may contain

covenants and other terms and provisions variously stated regarding the same or similar matters, and Debtor agrees that all such covenants, terms, and provisions are cumulative and all shall be performed and satisfied in accordance with their respective terms.

12. SEVERABILITY. If one or more provisions contained in this Agreement shall be invalid, illegal, or unenforceable in any respect in any jurisdiction or with respect to any party, such invalidity, illegality, or unenforceability in such jurisdiction or with respect to such party shall, to the fullest extent permitted by applicable law, not invalidate or render illegal or unenforceable any such provision in any other jurisdiction or with respect to any other party, or any other provisions of this Agreement.

13. NOTICES. All notices and other communications hereunder shall be in writing and shall be mailed, sent, or delivered in accordance with the Credit Agreement.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement, as of the date first above written.

DEBTOR

Date: _ _ _ _ _ _

_ _[*NAME OF DEBTOR*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

SECURED PARTY

Date: _ _ _ _ _ _

_ _[*NAME OF SECURED PARTY*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

© The Regents of the University of California

G. Convertible Promissory Notes

§16.34 1. Generally

Convertible promissory notes are often used to enable a company to obtain funds and a lender to invest in the company at a time when the company does not have an open round of equity financing available. They may also be used as bridge financing by start-up companies that need capital and have a potential equity investor, but that do not wish to commit in advance to the specific terms to be offered in the next round of equity financing because all participants have not been identified. When the terms of the next round are fixed, the debt will convert to the equity offered in that round. Convertible debt may also be a way for an angel investor or friend or family member to contribute funds to the company at an early stage as debt, and later on to take advantage of the leverage that future investors may have in structuring a future round of equity financing with preferential terms.

NOTE: A promissory note convertible into an equity security will be treated as a security for the purposes of federal and state securities laws, so appropriate exemptions from registration must be identified and complied with. See generally 15 USC §§77a-77aa; Corp C §25019; Financing and Protecting California Businesses (Cal CEB 2006).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/16 Financing an Online Business/§16.35 2. Form: Convertible Promissory Note

§16.35 2. Form: Convertible Promissory Note

To download **Word** version, right click and choose *Save Target As*

To download **WordPerfect** version, right click and choose *Save Target As*

CONVERTIBLE PROMISSORY NOTE

THIS NOTE AND ANY SHARES THAT MAY BE ISSUED ON THE CONVERSION OF THIS NOTE HAVE BEEN ACQUIRED FOR INVESTMENT AND HAVE NOT BEEN REGISTERED UNDER THE SECURITIES ACT OF 1933, AS AMENDED, OR REGISTERED OR QUALIFIED UNDER ANY STATE SECURITIES LAWS. NEITHER THIS NOTE NOR ANY PORTION HEREOF OR INTEREST HEREIN MAY BE SOLD, ASSIGNED, TRANSFERRED, PLEDGED, OR OTHERWISE DISPOSED OF UNLESS THE SAME IS REGISTERED UNDER SAID ACT AND APPLICABLE STATE SECURITIES LAWS, OR UNLESS AN EXEMPTION FROM SUCH REGISTRATION IS AVAILABLE AND THE COMPANY SHALL HAVE RECEIVED, AT THE EXPENSE OF THE HOLDER HEREOF, EVIDENCE OF SUCH EXEMPTION REASONABLY SATISFACTORY TO THE COMPANY (WHICH MAY INCLUDE, AMONG OTHER THINGS, AN OPINION OF COUNSEL REASONABLY SATISFACTORY TO THE COMPANY).

_ _[*Dollar amount*]_ _
_ _[*Date*]_ _
_ _[*City*]_ _, *California*

FOR VALUE RECEIVED, _ _[*name*]_ _ (the "Company") hereby promises to pay to the order of _ _[*name*]_ _ (the "Holder"), or assigns, at _ _[*address*]_ _, or at such other office or agency as the Holder has designated to the Company in writing, the principal sum of _ _[*dollar amount*]_ _, together with interest on such principal sum at the rate provided herein.

1. MATURITY DATE. Subjection to conversion under Section 3 hereof, the outstanding principal balance hereof will be due and payable in full on the _ _[*e.g., fifth*]_ _ anniversary of the date of this Note (the "Maturity Date").

2. INTEREST. Interest shall accrue on the unpaid principal balance of this Note (the "Outstanding Balance") at a rate equal to the lower of (a) 10% per annum, or (b) the highest rate permitted by applicable law, compounded annually on the basis of a 365-day year, commencing on the date hereof. Interest on the Outstanding Balance shall be payable in a single payment on the earlier of (a) the Maturity Date, or (b) the conversion of this Note in accordance with Section 3 hereof.

3. CONVERSION. Before the Maturity Date (or on the Maturity Date, in the event of conversion under Section 3.2 hereof), the Outstanding Balance of this Note and any accrued but unpaid interest thereon shall be payable by conversion of this Note as follows:

3.1. AUTOMATIC CONVERSION ON QUALIFIED FINANCING. If the Company closes a Qualified Financing (as defined at the end of this paragraph) before the Maturity Date, then all accrued and unpaid interest and the Outstanding Balance under this Note shall be converted automatically into the shares issued in such Qualified Financing ("Financing Conversion Securities") at a conversion price equal to _ _[*number*]_ _% of the purchase price per share of the Financing Conversion Securities paid by the investors in the Qualified Financing. Such conversion shall be deemed to have been effected on the date of closing the Qualified Financing. The Company shall deliver to the Holder one or more stock certificates representing the shares of Financing Conversion Securities into which this Note is converted as soon as practicable after the conversion. On conversion under this Section, this Note shall be deemed to be paid in full and shall automatically be cancelled. The Company shall provide the Holder with notice of a proposed Qualified Financing at least 10 days before the proposed closing date of such financing. A "Qualified Financing" shall mean the closing of an investment or series of investments in the Company occurring after the date hereof and before the Maturity Date (excluding the issuance or conversion of this Note or any notes containing substantially similar terms as this Note) in which the Company receives from one or more institutional investors (including "angel" investors) gross proceeds of at least _ _[*dollar amount*]_ _ in exchange for equity securities of the Company.

Comment: Conversion can be automatic or optional. This promissory note includes both types (automatic in Section 3.1, optional in Section 3.2). Under Section 3.1, automatic conversion is triggered by a subsequent financing that meets or exceeds a stated dollar threshold. The lender will want the dollar threshold to operate in the aggregate, so that a series of smaller transactions cannot be used to circumvent the automatic conversion feature. Care should be taken to

ensure that inapplicable transactions are carved out of the calculation of the trigger amount. Here, other similar convertible promissory notes do not count towards the total. Note that the specific type of equity that this note will convert into is not specified, because the note will convert into whatever form of equity is offered in the Qualified Financing.

3.2. OPTIONAL CONVERSION. If a Qualified Financing has not occurred by the Maturity Date, on the Holder's election by notice in writing to the Company not later than the Maturity Date, all accrued and unpaid interest and the Outstanding Balance under this Note shall be converted into common stock of the Company (the "Common Stock") at a conversion price equal to the fair market value per share of Common Stock determined as of a date just before any such conversion. For purposes of this Agreement, the fair market value per share shall be determined by the Board of Directors of the Company in good faith. The Company shall deliver to the Holder one or more stock certificates representing the shares of Common Stock into which this Note is converted as soon as practicable after the conversion. On a conversion under this Section, this Note shall be deemed to be paid in full and shall automatically be cancelled.

Comment: This optional conversion provision permits the lender to have an "out" if a qualified equity financing does not occur by the stated maturity date. Under this provision, the note will convert into common stock of the company.

4. ISSUANCE OF CONVERSION SECURITIES OR COMMON STOCK. Anything to the contrary in this Note notwithstanding, the Company's obligation to issue Financing Conversion Securities or Common Stock to Holder hereunder is expressly conditioned on compliance of such issuance with applicable federal and state securities laws without registration or other qualification thereunder.

5. HOLDER'S RIGHTS. Before the conversion and issuance of any Financing Conversion Securities or Common Stock under this Note, the Holder of this Note will not have any rights as a shareholder of the Company.

6. COMPLIANCE WITH SECURITIES LAWS. This Note may not be transferred in the absence of registration or other qualification under federal and applicable state securities laws, or valid and perfected exemptions from those laws.

7. NOTICES. Notice of demand for payment of this Note, and any other notices or communications given hereunder or in connection herewith, shall be given by first class mail or personal delivery and become effective 3 days after proper posting, or on actual receipt in the event of personal delivery or confirmed transmission by facsimile (a) to Company, at its principal executive offices, and (b) to the Holder, at the address provided by the Holder to the Company.

8. WAIVERS. The Company hereby waives presentment for payment, notice of nonpayment, and protest.

9. SEVERABILITY. If all or part of any provision of this Note shall for any reason be held to be invalid, illegal, or unenforceable in any respect, such invalidity, illegality, or other unenforceability shall not affect any other provision (or the remaining part of the affected provision) hereof, but this Note shall be construed as if such invalid, illegal, or unenforceable provision (or part thereof) had never been contained in this Note, but only to the extent that such provision is invalid, illegal, or unenforceable.

10. GOVERNING LAW. This Note is made and delivered in California and shall be governed by the laws of the State of California.

IN WITNESS WHEREOF, the Company has caused this Note to be executed as of the date first above written.

Date: _ _ _ _ _ _

_ _[*NAME OF COMPANY*]_ _,
a _ _[*state of incorporation*]_ _ **corporation**

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

_ _[*Company's address*]_ _

© The Regents of the University of California

17

Advertising on the Internet

I. INTERNET ADVERTISING REGULATION
A. Introduction §17.1
B. Overview of Applicable Laws §17.2
1. Lanham Act §17.3
2. Federal Trade Commission Act §17.4
a. FTC's Dot Com Disclosure Guidelines §17.5
b. Liability for Deceptive Advertising; FTC Enforcement Actions §17.6
c. Examples of FTC Enforcement Actions §17.7
d. Endorsements and Testimonials §17.7A
3. State Laws §17.8
a. Laws Prohibiting False or Misleading Advertising Generally §17.9
b. Laws Regulating Telephone, Internet, and Catalog Sales §17.10
C. Attorney Internet Advertising
1. Overview §17.10A
2. California Rules of Professional Conduct §17.10B
3. ABA Model Rules of Professional Conduct §17.10C
4. ABA Best Practice Guidelines for Legal Information Providers §17.10D
D. Unsolicited E-Mail ("Spam") §17.11
1. Federal Legislation: CAN-SPAM Act
a. Generally §17.12
b. E-Mail Subject to CAN-SPAM Act §17.13
c. CAN-SPAM Act: Basic Requirements for Commercial E-Mail Messages §17.14
(1) Identification as Advertisement §17.15
(2) Notice and Opt-Out Mechanism §17.16
(3) Postal Address §17.17
(4) Affirmative Consent §17.18
(5) Forwarding Commercial E-Mails §17.18A
d. Deceptive E-Mail Practices §17.19
e. Sexually Oriented Materials §17.20
f. Attribution Rules §17.21
g. Enforcement of CAN-SPAM §17.22
h. National "Do Not E-Mail" Registry §17.23
i. Commercial E-Mails Sent to Wireless Devices §17.23A
j. Criminal Liability Under CAN-SPAM §17.23B
2. State Anti-Spam Laws
a. Generally §17.24
b. California Anti-Spam Laws §17.25
c. Scope of Preemption of California Law by CAN-SPAM Act §17.26
d. Penal Code §502(c) §17.27
3. Anti-Spam Litigation §17.28
4. Practical Methods of Blocking Spam E-Mail §17.29
E. Search Engine Optimization
1. Overview §17.29A
2. Optimization Tools and Techniques §17.29B

II. INTERNET ADVERTISING AGREEMENTS
A. Overview §17.30
B. Banner Advertising §17.31
C. Form: Banner Advertising Agreement §17.32
D. Internet Service Directories or Referral Sites §17.33
E. Form: Internet Advertising Agreement §17.34
F. Portal Agreements §17.35
G. Form: Interactive Marketing Agreement §17.36

© The Regents of the University of California

I. INTERNET ADVERTISING REGULATION

§17.1 A. Introduction

Sections 17.2-17.29 review applicable federal and California state laws and regulations and factors that should be considered when companies use e-mail or Internet advertisements to advertise their businesses. Advertisements and other content made available online can reach users anywhere in the world. As a result, California businesses should understand that their advertising and business efforts may implicate the laws of other states and countries. To the extent that a company is directly targeting users or seeking advertisers in other states or countries, the company should familiarize itself with applicable laws of those jurisdictions. This becomes increasingly important as a business increases its contacts—*e.g.,* customers, employees, offices—in a particular location. Sections 17.11-17.29 review the laws regulating unsolicited e-mail advertisements, more commonly known as "spam."

Generating commercial sales online begins with creation of a website. Once the website is operating, the site can be promoted and advertised online in a variety of ways, *e.g.,* through banner advertisements on a third party's website (see §§17.31-17.32), pop-up advertisements (ads in windows superimposed over the web page a user is trying to view); metatags (see §§3.71-3.76), mass e-mail messages (see §§17.11-17.29), linking arrangements (see §§8.14-8.18), and co-branding arrangements (see §§11.6-11.7). This chapter addresses the legal framework that applies to these advertising and promotional efforts.

© The Regents of the University of California

§17.2 B. Overview of Applicable Laws

Regulation of online advertising is a combination of old and new—old laws being applied to new technologies and new laws emerging in an effort to regulate new technology where old laws have not succeeded. Certain provisions of the Lanham Act (15 USC §§1051-1141n), the Federal Trade Commission Act (15 USC §§41-58) (the FTC Act), and the California Business and Professions Code are directed to advertising. Laws governing copyrights and rights of publicity may be also implicated by online advertising activities. See §§1.1-1.23, 20.9.

© The Regents of the University of California

§17.3 1. Lanham Act

The Trademark Act of 1946 (also known as the Lanham Act) (15 USC §§1051-1141n), is the federal law providing for registration of trademarks, service marks, trade names, and trade dress; it also creates liability for infringement of registered marks (see generally §§3.60-3.70). False advertising claims may be brought under the Lanham Act. Unlike the FTC Act (see §§17.4-17.7), the Lanham Act creates a private cause of action against persons engaging in false advertising (15 USC §1125(a)(1)):

> [A]ny person who, on or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of act, or false or misleading misrepresentation of fact… shall be liable to civil action by any person who believes that he or she is or is likely to be damaged by such act.

Some commentators have suggested that bringing an action for false advertising under the Lanham Act may be difficult. See, *e.g.,* Burns, *Confused Jurisprudence: False Advertising Under the Lanham Act*, 79 BUL Rev 807 (Oct. 1999). In fact, case law does not reflect many successful claims under 15 USC §1125(a)(1).

Other aspects of the Lanham Act may be implicated in online advertising, however. For example, words used to key or link banner advertisements (see §17.31) to particular Internet search results may infringe a competitor's trademarks. See generally *Playboy Enters. v Netscape Communications Corp.* (9th Cir 2004) 354 F3d 1020 (triable issue of fact whether defendants' use of the words "playboy" and "playmate" as links for general adult entertainment advertising infringed the plaintiff's marks); Shea, *Trademarks and Keyword Banner Advertising*, 75 S Cal L Rev 529 (2002). Further, a chosen domain name may lead to a claim of infringement when the chosen name is confusingly similar to a trademark used by another company, particularly if the other company sells goods or services that are similar, and if both companies use the Internet as a marketing channel. When these three factors (known in Ninth Circuit case law as the "Internet Trinity") are present, even a website disclaimer may not suffice to overcome a claim of trademark infringement. See *SMC Promotions, Inc. v SMC Promotions* (CD Cal 2005) 355 F Supp 2d 1127; see also *Interstellar Starship Servs., Ltd. v EPIX, Inc.* (9th Cir 2002) 304 F3d 936, 942 (describing "Internet Trinity" of factors for determining likelihood of confusion).

© The Regents of the University of California

§17.4 2. Federal Trade Commission Act

Under the Federal Trade Commission Act (FTC Act) (15 USC §§41-58), the Federal Trade Commission (FTC) has jurisdiction over most, although not all, advertising on the Internet. The FTC has only limited jurisdiction over advertising involving commerce with foreign nations. 15 USC §45(a)(3). Further, the FTC does not have jurisdiction over banks, certain savings and loan institutions, federal credit unions, common carriers, domestic and foreign air carriers, and persons, partnerships, or corporations subject to the Packers and Stockyards Act (7 USC §§181-229b). 15 USC §45(a)(2).

The FTC Act provides that the FTC is "empowered and directed to prevent" persons and certain entities from using unfair methods of competition "in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce." 15 USC §45(a)(2). The FTC Act's prohibition on "unfair or deceptive acts or practices" generally covers advertising claims, marketing and promotional activities, and sales transactions, and is not limited to any particular medium. See 15 USC §45. The same rules that apply to advertising in other media and to consumer transactions also apply on the Internet. In general, any form of advertising must be truthful and not mislead consumers. A claim can be misleading if relevant information is left out or if the claim implies something that is not true. See FTC Policy Statement on Deception (Deception Policy Statement), appended to *Cliffdale Assocs., Inc.* (1984) 103 FTC 110, 174.

The FTC Act also requires that advertising claims be substantiated, especially when they concern health, safety, or performance. The type of evidence required depends on the product, the claims, and what experts believe is necessary. See FTC Policy Statement on Advertising Substantiation, appended to *Thompson Med. Co.* (1984) 104 FTC 648, 839, aff'd (DC Cir 1986) 791 F2d 189, cert denied (1987) 479 US 1086. Sellers are responsible for claims they make about their products and services. Third parties, such as advertising agencies or website designers, may also be liable for making or disseminating deceptive representations if they participate in the preparation or distribution of deceptive advertising, or are aware of the deceptive claims. See *Standard Oil Co. v FTC* (9th Cir 1978) 577 F2d 653.

PRACTICE TIP: Counsel should advise companies doing business on the Internet to make sure that all advertising claims are substantiated. Companies that market or sell products manufactured by third parties should request and review documents and other materials that substantiate advertising claims, rather than merely repeating what the manufacturer says about the product.

© The Regents of the University of California

§17.5 a. FTC's Dot Com Disclosure Guidelines

The FTC has published guidelines to help online businesses determine whether an advertisement would be considered unfair or deceptive. See "Dot Com Disclosures" at http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus41.pdf. Under these guidelines, an advertising claim may be considered misleading if relevant information is omitted or if the claim is not true. To prevent advertisements from being misleading, advertisers may need to add certain qualifications or disclosures to the text of the ad. The disclosures must be set forth clearly and conspicuously. Factors considered in determining whether a disclosure is clear and conspicuous are placement (proximity to the claim it is qualifying), prominence, and the form of the disclosure (audio or written). The FTC's guidelines suggest how and where to place disclosures in online advertisements in order to meet the "clear and conspicuous" requirement (http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus41.pdf):

- Place the disclosure near, and if possible, on the same screen as the advertising claim. If scrolling is necessary to view the disclosure, use text or visual cues to encourage consumers to scroll down. If the screen is designed so that a consumer is not likely to scroll down, the disclosure could be deemed misleading.
- Place alerts so that consumers turn their attention to the disclaimer, such as "see below for important information on…."
- Delete unrelated information (graphics or text) that separates the claim from the disclosure.
- Avoid the use of hyperlinks for disclosures. If using a hyperlink, identify the link and make it obvious so that consumers are likely to click on it. Place it near the relevant advertising claim, and label it appropriately to convey its importance and the relevance of the information it leads to.
- The click-through web page should display the disclosures with no further click-throughs necessary. Assess the effectiveness of the hyperlink by monitoring click-through rates; make changes accordingly.
- Use clear language and syntax so that consumers understand the disclosures made.
- Prominently display disclosures so that they are noticeable, and evaluate the size, color, and graphic treatment of the disclosures in relation to other parts of the web page.

NOTE: In *In re Gateway, Inc.* (May 15, 2001) FTC File No. 992 3276, the FTC found that Gateway's disclosure of possible additional fees for Internet service was not sufficiently conspicuous. The fee disclosure was made in a footnote four pages after the page describing the service, in the eighth of eleven lines of disclosures in approximately four-point type at the bottom of the page.

- Review the entire advertisement to ensure that other elements—text, graphics, hyperlinks, or sound—do not distract consumers' attention from the disclosure.
- Avoid using pop-up windows, especially if the window disappears or if the user will be unable to access it easily.
- Consider technological limitations of certain browsers when placing disclosures.
- Disclosures should be made before the page on which orders are taken; disclosures placed only on the order page may be deemed inadequate.
- Make disclosures at least as large as the advertisement.
- Avoid colors that make it difficult to read the disclosure.
- Repeat disclosures as needed on lengthy websites and in connection with repeated claims.
- If audio claims are used, use audio disclosures (at equal volume).
- Display visual disclosures for a sufficient amount of time so that consumers will notice, read, and understand them.
- Disclose the person or entity sponsoring the advertisement if it is not clear.

Another helpful FTC publication for online businesses is "Advertising and Marketing on the Internet: Rules of the Road," available at http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus28.shtm.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/17 Advertising on the Internet/§17.6 b. Liability for Deceptive Advertising; FTC Enforcement Actions

§17.6 b. Liability for Deceptive Advertising; FTC Enforcement Actions

False or deceptive advertisements may trigger FTC enforcement actions or civil lawsuits, including:

- Agency orders to cease and desist, and penalties of up $11,000 for each violation while order is in effect (15 USC §45(*l*)-(m); 28 USC §2461, Note);
- Injunctions by federal district courts, with fines up to $11,000 for each violation of an order (15 USC §§45(*l*)-(m), 53, 54; 28 USC §2461, Note); or
- Civil lawsuits for refunds to consumers of actual damages (15 USC §57b(b)).

Consumer complaints assist the FTC in investigating fraud and may lead to an enforcement action by the FTC. Complaints may be submitted to the FTC's Bureau of Consumer Protection (16 CFR §310.7) by mail or at the FTC website, http://www.ftc.gov. There is no private right of action under the FTC Act. FTC enforcement efforts include monitoring the Internet for false or deceptive advertising claims. FTC investigations may be either public or nonpublic.

If the FTC believes a company has violated the FTC Act, the FTC may propose that the company enter into a consent order. A company entering into a consent order is not required to admit that it violated the law, but it must agree to cease all activities described in the consent order. 16 CFR §2.32. If the company declines to sign a consent order, the FTC may initiate an administrative proceeding. The administrative law judge who hears the case may issue a cease and desist order or other relief if the company is found to have violated the FTC Act. 15 USC §45(b). The initial decision by the administrative law judge may be appealed to the FTC itself; decisions by the FTC are appealable to the appropriate U.S. court of appeals. 15 USC §45(c).

If a company violates a consent order, the FTC may seek civil penalties or an injunction against the company. 15 USC §45(*l*). More information on FTC complaint procedures is available at http://www.ftc.gov/ftc/action.htm.

In cases of fraud or other serious misconduct, the FTC can go directly to court to seek injunctive and other relief, including civil penalties and any ancillary relief necessary to achieve justice. 15 USC §§53-54, 57b. This authority includes the power to compel disgorgements of profits and the power to order consumer redress. *FTC v Gem Merchandising Corp.* (11th Cir 1996) 87 F3d 466, 470.

© The Regents of the University of California

§17.7 c. Examples of FTC Enforcement Actions

The FTC has initiated many enforcement actions related to online advertising, including advertisements for business opportunities, cash grants, rebates, weight loss programs, and cellulite creams; claims of goods advertised but not delivered; complaints about promotions of healthcare products; complaints about the safety of products; and claims of misrepresentation about an advertiser's ability to repair credit. Following are examples of some recent FTC actions:

- *FTC v Myricks d/b/a MP3DownloadCity.com* (CD Cal 2006, Civ Action No. CV-05-7013) available at http://www.ftc.gov/os/caselist/cv057013/cv057013.htm (website operator who deceptively claimed its web service would permit subscribers to legally download copyrighted materials ordered to notify customers of falsity of prior claims of legality; to disclose liability risks of sharing copyrighted material without permission; to refund more than $15,000 to customers who purchased memberships; and to cease making misrepresentations about peer-to-peer file-sharing products or services).
- *FTC v Vital Dynamics, Inc.* (Dec. 26, 2002) FTC File No. 012 3249 (California company and its officers marketing "breast enhancement product" liable for failure to substantiate claims made with respect to product).
- *FTC v Zuccarini* (ED Pa, Apr. 10, 2002, No. 01-CV-4854) 2002 US Dist Lexis 13324 (respondent permanently enjoined from obstructing consumers' access to desired web destinations by redirecting them through series of advertisements to his own websites and preventing them from exiting his sites ("mousetrapping" them)).
- *In re Esrim Ve Sheva Holding Corp.* (Dec. 17, 2001) FTC File No. 012 3116 (respondent ordered to refrain from making unsubstantiated claim that product called "SuperFuelMAX" provided great fuel savings and reduced fuel emissions).
- *FTC v Salyon, Inc.* (Nov. 6, 2001) FTC File No. 01 23124 (respondent ordered to refrain from promising to improve customers' credit histories and marketing credit cards without disclosing substantial limits on use of cards).
- *In re Gateway, Inc.* (May 15, 2001) FTC File No. 992 3276 (Gateway ordered not to misrepresent cost of Internet service and required to make clear and conspicuous disclosures of fees; company also required to refund all charges paid by consumers before company clarified limitations on "toll free" calling).

FTC case files are indexed by month and year at http://www.ftc.gov/os/actions.shtm.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/17 Advertising on the Internet/§17.7A d. Endorsements and Testimonials

§17.7A d. Endorsements and Testimonials

The FTC has revised its Guides Concerning the Use of Endorsements and Testimonials in Advertising. 16 CFR §§255.0-255.5. The revisions include bloggers as marketers required to disclose material connections to advertisers. See http://www.ftc.gov/os/2008/11/P034520endorsementguides.pdf and http://www.ftc.gov/multimedia/video/business/endorsement-guides.shtm. The Guides define endorsements as synonymous with testimonials (16 CFR §255.0(b)):

> [A]n endorsement means any advertising message (including verbal statements, demonstrations, or depictions of the name, signature, likeness or other identifying personal characteristics of an individual or the name or seal of an organization) that consumers are likely to believe reflects the opinions, beliefs, findings, or experiences of a party other than the sponsoring advertiser, even if the views expressed by that party are identical to those of the sponsoring advertiser.

Endorsements "must reflect honest opinions, findings, beliefs or experience of the endorser" and "cannot convey any express or implied representations that would be deceptive if made directly by the advertiser." 16 CFR §255.1(a). Advertisers are subject to liability for false or unsubstantiated statements made through endorsements, and endorsers also may be liable for statements made in the course of their endorsements. 16 CFR §255.1(c). See, *e.g.,* 16 CFR §255.1, Example 5.

If a connection exists between an endorser and the seller of the advertised product that might materially affect the weight or credibility of the endorsement, the connection must be fully disclosed. 16 CFR §255.5. The FTC provides examples of connections that include conduct such as payment for endorsement services, receipt of free products, eligibility for prizes, or employment of the endorser by the manufacturer of the product or the provider of the service being endorsed. See, *e.g.,* 16 CFR §255.5, Example 7:

> A college student who has earned a reputation as a video game expert maintains a personal weblog or "blog" where he posts entries about his gaming experiences. Readers of his blog frequently seek his opinions about video game hardware and software. As it has done in the past, the manufacturer of a newly released video game system sends the student a free copy of the system and asks him to write about it on his blog. He tests the new gaming system and writes a favorable review. Because his review is disseminated via a form of consumer-generated media in which his relationship to the advertiser is not inherently obvious, readers are unlikely to know that he has received the video game system free of charge in exchange for his review of the product, and given the value of the video game system, this fact likely would materially affect the credibility they attach to his endorsement. Accordingly, the blogger should clearly and conspicuously disclose that he received the gaming system free of charge. The manufacturer should advise him at the time it provides the gaming system that this connection should be disclosed, and it should have procedures in place to try to monitor his postings for compliance.

Section 255.0 states that

> [p]ractices inconsistent with these Guides may result in corrective action by the Commission under Section 5 if, after investigation, the Commission has reason to believe that the practices fall within the scope of conduct declared unlawful by the statute.

The civil penalty for unfair or deceptive acts under §5 of the Federal Trade Commission Act (FTC Act) (15 USC §45) is $16,000. 16 CFR §1.98.

PRACTICE TIP: If a blogger receives money or any value, such as a free product, from the entity whose product is being reviewed, even if unsolicited, the blogger must make a disclosure and the disclosure must be viewable by readers of the review. It does not matter whether the review is positive or negative. See 16 CFR §255.2. If any value has been received from the advertiser, the blogger should actually use the product or service in question before reviewing it or the review may be deemed to be deceptive.

© The Regents of the University of California

§17.8 3. State Laws

Online businesses operating out of California must also comply with state laws concerning false or misleading advertising. California's primary law on false advertising is Bus & P C §17500. See §17.9. Cyberpiracy is addressed in Bus & P C §§17525-17528, and numerous sections of the Business and Professions Code, including §17500, have been amended to include the Internet among the media by which dissemination of false information about products and services is prohibited. See Stats 1998, ch 599. Business and Professions Code §17538 regulates the terms and conditions of telephone, Internet, and catalog sales, and includes requirements for the text of website advertisements and product offerings. See §17.10.

© The Regents of the University of California

§17.9 a. Laws Prohibiting False or Misleading Advertising Generally

Business and Professions Code §17500 broadly prohibits "any person" from disseminating, by any means, any "untrue or misleading" statement in connection with the sale of property or services. "Person" includes business entities as well as natural persons. Bus & P C §17201. "[A] statement is false or misleading if members of the public are likely to be deceived. Intent of the disseminator and knowledge of the customer are both irrelevant." *Chern v Bank of America* (1976) 15 C3d 866, 876, 127 CR 110. Particular sections of the Business and Professions Code address advertising of specific kinds of goods or services, *e.g.,* Bus & P C §§6157-6159.2 (legal advertising), 17510-17510.95 (charitable solicitations), and 17511-17513 (telephone sales). In addition, there are special rules for contests and sweepstakes (Bus & P C §§17539-17539.6).

The state can seek civil remedies for violations (see Bus & P C §§17200, 17206), and private individuals may seek injunctive or equitable relief (Bus & P C §17204). The plaintiff bears the burden of proving defendant's advertising claims false. Bus & P C §17508(f). See also *National Council Against Health Fraud, Inc. v King Bio Pharms., Inc.* (2003) 107 CA4th 1336, 133 CR2d 207.

The California Department of Consumer Affairs (DCA) is responsible for advertising regulation in California. See generally Bus & P C §§300-313.5. The DCA uses the following factors to determine whether an advertisement is deceptive or misleading: (1) the total impression left by the advertisement, including statements said and assertions implied; (2) failure to disclose material facts; (3) whether the advertisement can be interpreted in multiple ways; (4) exaggerations if the claim appears factually based; and (5) failure to substantiate a claim. Even an advertisement that is ambiguous, partially true, or sometimes even literally true may violate Bus & P C §17500. The DCA website gives a number of helpful examples of advertising that would violate the Business and Professions Code, such as "bait and switch" techniques, inadequate supplies of advertised items, deceptive use of the phrase "Made in the U.S.A.," and inadequate disclosure of sales prices. See http://www.dca.ca.gov/publications/advfact.shtml.

The California Consumers Legal Remedies Act (CC §§1750-1784) also applies to advertising. Among its prohibitions are:

- Misrepresenting the source, sponsorship, approval, certification, or quality of goods or services (CC §1770(a)(2));
- Advertising goods or services with the intent not to sell them as advertised (CC §1770(a)(9));
- Making false or misleading statements of fact relating to the existence of or amount of price reductions (CC §1770(a)(13));
- Representing that a transaction involves rights, remedies, or obligations that are not involved or are prohibited by law (CC §1770(a)(14)); and
- Misrepresenting a salesperson's authority to negotiate final terms of a consumer transaction (CC §1770(a)(18)).

Out-of-state Internet vendors must also take care to comply with California's advertising laws. In *People ex rel Brown v PuriTec* (2007) 153 CA4th 1524, 64 CR3d 270, the court determined that a Nevada company had violated a California advertising law by making health-related claims online for water treatment devices that were not certified by the California Department of Health Services. The court held that the application of California advertising law to the Nevada-based Internet vendor was constitutional, and required the website operator to inform California customers that its devices are not certified by the State of California and that no health or safety claims about the drinking water could be made under California law. 153 CA4th at 1532. The court rejected an argument that this would require the creation of multiple websites targeted for separate states, suggesting that the notice to California customers could be placed on the "Check-Out" page. 153 CA4th at 1532.

© The Regents of the University of California

§17.10 b. Laws Regulating Telephone, Internet, and Catalog Sales

Business and Professions Code §17538 regulates the terms and conditions of telephone, Internet, mail order, and catalog sales, and includes detailed notice and disclosure requirements that may affect the text of online advertisements and product offerings. Section 17538 applies to out-of-state vendors if the sales transaction involves a California buyer. Bus & P C §17538(d). In general, the statute prohibits any vendor from accepting payment for goods or services ordered by telephone, mail, or through the Internet, and then—unless otherwise conspicuously stated in the product advertisement or offering—allowing 30 days to elapse without doing any one of the following (Bus & P C §17538(a)):

- Shipping the goods or services ordered;
- Refunding the purchase price or crediting the buyer's account;
- Notifying the buyer of the delay and offering to refund the price paid; or
- Shipping substitute goods or services of equivalent or superior quality, provided that the buyer is given the opportunity to return the substituted goods or services and obtain a refund.

Vendors taking orders over the Internet must disclose the legal name and street address of their business and their return and refund policy before accepting any payment or processing any debit or credit charge from a customer. Bus & P C §17538(d)(1). There are detailed requirements concerning the format and placement of these disclosures on the vendor's website. See Bus & P C §17538(d)(2). Violation of any provision of Bus & P C §17538 is a misdemeanor punishable by a fine of up to $1000, by imprisonment in the county jail for up to 6 months, or both. Bus & P C §17538(g).

© The Regents of the University of California

C. Attorney Internet Advertising

§17.10A 1. Overview

Attorneys who advertise their services on the Internet should consider both national and state ethics rules when designing websites and corresponding with clients or prospective clients online. California practitioners must comply with the California Rules of Professional Conduct (see §17.10B) when advertising legal services on the Internet. Attorneys should also be aware of the ABA Model Rules of Professional Conduct (see §17.10C), available at http://www.abanet.org/cpr/mrpc/mrpc_toc.html, which serve as a pattern for ethical rules in many states outside California. In addition, publishers of legal information websites are encouraged to adhere to the ABA Best Practices for Legal Information Web Site Providers, available at http://www.abanet.org/elawyering/tool/practices.shtml. See §17.10D.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/17 Advertising on the Internet/§17.10B 2. California Rules of Professional Conduct

§17.10B 2. California Rules of Professional Conduct

California attorneys must comply with state ethics rules when advertising or promoting legal services online. Internet advertising regulations are contained in Cal Rules of Prof Cond 1-400; Article 9.5 (Legal Advertising) of the State Bar Act (Bus & P C §§6157-6159.2); and advisory opinions published by the State Bar of California at http://calbar.ca.gov/state/calbar/calbar_generic.jsp?cid=10133&id=1129.

California lawyers should consider the following when creating and maintaining a professional website:

- Advertisements must not be false or misleading, and should be factually substantiated. Cal Rules of Prof Cond 1-400(C).
- A copy of all advertisements must be kept for two years. Cal Rules of Prof Cond 1-400(F).
- Attorney websites are generally considered communications and not solicitations within the meaning of Cal Rules of Prof Cond 1-400(A). State Bar Formal Opinion No. 2001-155.
- Attorneys are advised to use disclaimers on websites to prevent jurisdictional problems. Suggested disclaimers state that the attorney is advertising only in California and does not seek to represent someone based solely on a visit to the site. The website should also set forth the areas of law practiced by the attorney, the location of the attorney's office, and the jurisdictions in which the attorney is licensed.
- California attorneys who are licensed or have offices in other states should take steps to ensure that their websites comply with ethics regulations in those states. State Bar Formal Opinion No. 2001-155.
- Attorneys with websites that contain an e-mail address or communication forms may effectively disclaim that they owe a duty of confidentiality to visitors only if the disclaimer states in a plain language reference that any submissions to the attorney are not confidential. Note that it is not enough simply to have a visitor agree that no attorney-client relationship or confidential relationship has been formed. State Bar Formal Opinion No. 2005-168.
- Communications with prospective clients in a chat room are not prohibited "solicitations," but lawyers should be careful to avoid violating other ethics regulations. For example, attorney participation in a mass disaster victim chat room violates regulations preventing communications that intrude or cause duress. State Bar Formal Opinion No. 2004-166.

See Cal Rules of Prof Cond 1-400 and the Rules of the State Bar of California, available at http://calbar.ca.gov/state/calbar/calbar_generic.jsp?BV_SessionID=1549191326.1235085934&BV_EngineID=cccfadegfmdjijgcfngcfkmdffidfnf.0&id=33461&cid=14045, for additional guidance.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/17 Advertising on the Internet/§17.10C 3. ABA Model Rules of Professional Conduct

§17.10C 3. ABA Model Rules of Professional Conduct

California attorneys who advertise on the Internet or who are considering soliciting business online should also be aware of the following general principles stated in the ABA Model Rules of Professional Conduct:

- False or misleading statements are prohibited. ABA Model Rules of Prof Cond 7.1.
- The advertisement must contain the name of at least one lawyer responsible for its content. ABA Model Rules of Prof Cond 7.2(c).
- A lawyer may not solicit professional employment for profit by a real-time electronic contact with a prospective client. ABA Model Rules of Prof Cond 7.3(a).
- Electronic communication from a lawyer soliciting employment from a prospective client known to be in need of legal services shall include the words "Advertising Material" at the beginning and ending of any recorded or electronic communication. ABA Model Rules of Prof Cond 7.3(c).

The ABA Model Rules of Professional Conduct, which serve as a model for ethical rules in many states outside California, are available at http://www.abanet.org/cpr/mrpc/mrpc_toc.html.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/17 Advertising on the Internet/§17.10D 4. ABA Best Practice Guidelines for Legal Information Providers

§17.10D 4. ABA Best Practice Guidelines for Legal Information Providers

The ABA Best Practice Guidelines were developed to provide guidance to legal website developers and to promote the development of quality legal websites. The guidelines are available at http://www.abanet.org/elawyering/tool/practices.shtml. Although it is suggested that legal websites adhere to these guidelines, the guidelines do not have the force of law.

© The Regents of the University of California

§17.11 D. Unsolicited E-Mail ("Spam")

Millions of unsolicited commercial e-mail messages (known colloquially as "spam") are sent daily, often by senders who have taken steps to conceal their identities. Spam has become one of the biggest problems facing Internet users and Internet service providers (ISPs). Costs associated with spam include ISP costs for storage and processing; the recipient's time (and associated ISP charges) to review and delete it; and the risk of loss of legitimate e-mail messages among the larger volume of spam. ISPs may also incur costs to implement spam-blocking software, to process and respond to subscriber complaints, and to determine where to reroute spam if a false return e-mail address is used. In addition, much spam is offensive to recipients. Both Congress and state legislatures have recognized that unsolicited e-mail constitutes a burden on the Internet, and have enacted legislation that restricts spam.

ISPs have been successful in blocking spammers partly because spamming is considered commercial speech, and is therefore afforded a lower level of protection by the First Amendment. *Florida Bar v Went For It, Inc.* (1995) 515 US 618, 623, 132 L Ed 2d 541, 549, 115 S Ct 2371. Moreover, ISPs are private rather than governmental entities and are not subject to the First and Fourteenth Amendments.

Effective January 1, 2004, Congress adopted the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act), codified primarily in 15 USC §§7701-7713. See §§17.12-17.23. The Federal Trade Commission (FTC) has primary responsibility for enforcing the CAN-SPAM Act. In addition, the FTC may bring enforcement actions against spammers under other provisions of the FTC Act. 15 USC §§41-58. See http://www.ftc.gov. Many states, including California, have also enacted statutes regulating unsolicited commercial e-mail and are now wrestling with the question of whether those statutes should be maintained in the face of possible preemption by the CAN-SPAM Act. See §§17.24-17.27.

© The Regents of the University of California

1. Federal Legislation: CAN-SPAM Act

§17.12 a. Generally

The federal anti-spam law—the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (better known by its acronym, the CAN-SPAM Act (Pub L 108-187, 117 Stat 2699, codified primarily in 15 USC §§7701-7713 and 18 USC §1037) is intended to preempt most state legislation regulating commercial e-mail, including most of the California anti-spam law discussed in §17.25. Rules under the Act are found at 16 CFR §§316.1-316.6.

Compared with some previous state legislative efforts (see §17.25), the CAN-SPAM Act is extremely permissive. Rather than generally prohibiting spam, it adopts an "opt-out" approach. Although the Act prohibits using false headers, falsifying the sender's identity, and other deceptive e-mail practices, the Act broadly allows unsolicited commercial e-mail, provided that the e-mail message:

- Is identified as an advertisement;
- Provides an "opt-out" mechanism; and
- Includes the sender's physical postal address.

These requirements are discussed in more detail in §§17.14-17.17.

The FTC) is given authority to promulgate regulations implementing the Act. 15 USC §7711. Thus far, the agency has done so for determining the primary purposes of e-mail and for labeling commercial e-mail containing sexually oriented material. In December 2005, the FTC issued a report to Congress, required within 2 years after the Act's effective date, analyzing the effectiveness of the Act and assessing the need for further legislation. See 15 USC §7709. The report, *Effectiveness and Enforcement of the CAN-SPAM Act: A Report to Congress* (Dec. 2005), is available at http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf.

According to the report, the Act is effective both in requiring online marketers to adopt "best practices" for their commercial e-mail activities and in providing government agencies and ISPs with an additional enforcement tool for use against spammers. Although the FTC did not recommend additional legislation to modify the Act, it recommended adoption of legislation that would increase the FTC's ability to pursue spammers outside United States borders. The FTC also recommended continued education efforts to protect consumers from receiving and viewing sexually explicit spam, and continued improvement in anti-spam technology, particularly authentication technology that would hinder the ability of spammers to operate anonymously. See *Effectiveness and Enforcement of the CAN-SPAM Act: A Report to Congress* (Dec. 2005); see also *The US SAFE WEB Act: Protecting Consumers from Spam, Spyware and Fraud, a Legislative Recommendation to Congress* (June 2005), available at http://www.ftc.gov/reports/ussafeweb/USSAFEWEB.pdf (discussing act targeted at enforcing anti-spam and related laws beyond United States borders).

PRACTICE TIP: It is important for counsel advising companies that employ e-mail for advertising or other promotional or commercial purposes to stay abreast of the FTC's future regulatory activities under the CAN-SPAM Act and to review any new federal regulations under the Act, as well as any court decisions interpreting the Act.

© The Regents of the University of California

§17.13 b. E-Mail Subject to CAN-SPAM Act

The CAN-SPAM Act does not apply to all e-mail messages sent by a business or individual, but only to "commercial electronic mail messages," which the Act defines as (15 USC §7702(2)(A)):

> [A]ny electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose).

The "primary purpose" of an e-mail determines whether it is a "commercial electronic mail message" for purposes of the Act. A reference to a commercial entity or a link to the website of a commercial entity will not cause an e-mail to be classified as a commercial message unless the commercial advertisement or promotion of a product or service is the primary purpose of the e-mail. 15 USC §7702(2)(D). Any message that does not have commercial advertising or promotion as its "primary purpose" is therefore excluded from regulation under the Act.

The primary purpose of an e-mail containing both commercial and transactional content will be deemed commercial if (16 CFR §316.3):

- The message consists exclusively of the commercial advertisement or promotion of a commercial product or service (16 CFR §316.3(a)(1));
- The message contains both a commercial advertisement or promotion of a commercial product or service and other content, and a recipient reasonably interpreting the subject line of the message would likely conclude that the message contains a commercial advertisement or promotion of a commercial product or service (16 CFR §§316.3(a)(2)(i), 316.3(a)(3)(i));
- The message contains both a commercial advertisement or promotion of a commercial product or service and "transactional or relationship" content, and the message's transactional or relationship content does not appear, in whole or in substantial part, at the beginning of the message (16 CFR §316.3(a)(2)(ii)); or
- The message contains both a commercial advertisement or promotion of a commercial product or service and other content that is not "transactional or relationship" content, and a recipient reasonably interpreting the body of the message would likely conclude that the primary purpose of the message is a commercial advertisement or promotion of a commercial product or service (16 CFR §316.3(a)(3)(i)).

See *Aitken v Communications Workers of Am.* (WD Va 2007) 496 F Supp 2d 653, 668 (e-mails held to be commercial because promoting union representation constituted commercial speech under the First Amendment). The FTC rule also gives guidance on message content that qualifies as "transactional or relationship" content (see 16 CFR §316.3(c)), and incorporates an earlier FTC rule on "Sexually Explicit Labeling," described in §17.20.

CAN-SPAM expressly excludes "transactional or relationship messages" from the definition of commercial electronic mail messages. 15 USC §7702(2)(B). A "transactional or relationship" message is one for which the primary purpose is either to (15 USC §7702(17)(A)):

- Confirm or complete a commercial transaction that the recipient has previously agreed to enter into with the sender;
- Provide warranty, product recall, safety, or security information about a product or service used or purchased by the recipient;
- Furnish an account statement or notice of changes in an account, loan, subscription, membership, or similar ongoing commercial relationship with the recipient;
- Provide information related to an employment relationship with the recipient, such as employee benefit plan information; or
- Deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously entered into with the sender.

The FTC has authority to enlarge or reduce the categories of e-mail messages that will be treated as "transactional or relationship" messages for purposes of the Act. 15 USC §7702(17)(B).

NOTE: Although personal e-mails are not covered by the CAN-SPAM Act, businesses should be aware that the Act does not apply only to mass e-mailings. Even a single, targeted e-mail that qualifies as a "commercial electronic mail message" (and is not otherwise exempt under the Act) must comply with the Act's requirements concerning identification as an advertisement, opt-out procedures, and sender address information, as described in §17.14.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/17 Advertising on the Internet/§17.14 c. CAN-SPAM Act: Basic Requirements for Commercial E-Mail Messages

§17.14 c. CAN-SPAM Act: Basic Requirements for Commercial E-Mail Messages

For companies doing business online, the most important aspects of the CAN-SPAM Act are the provisions requiring inclusion of an identifier, an opt-out mechanism, and a physical address in all commercial e-mails. Section 5(a)(5) of the Act provides that it is unlawful for any person to transmit a commercial e-mail message unless the message includes (15 USC §7704(a)(5)):

- Clear and conspicuous identification that the message is an advertisement or solicitation (unless the recipient has given affirmative consent to receive the message) (see §§17.15, 17.18);
- Clear and conspicuous notice of the opportunity to decline to receive further commercial electronic mail messages from the sender (see §17.16); and
- A valid physical postal address of the sender (see §17.17).

NOTE: When more than one person's products, services, or website are advertised in a single e-mail, one "person" may be designated the sender for purposes of CAN-SPAM compliance. See 18 CFR §316.2(m). A person is "any individual, group, unincorporated association, limited or general partnership, corporation, or other business entity." 18 CFR §316.2(h).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/17 Advertising on the Internet/§17.15 (1) Identification as Advertisement

§17.15 (1) Identification as Advertisement

Commercial e-mails must contain a clear and conspicuous notice that the message is an advertisement or solicitation and that the recipient can opt out of receiving more commercial e-mail from the sender. 15 USC §7704(a)(5). The CAN-SPAM Act expressly prohibits the FTC from adopting any regulation requiring any specific words, characters, marks, or labels to identify the e-mail as an advertisement in any particular place in the message. 15 USC §7711(b). Thus, for the present, businesses are free to decide how to identify their commercial e-mails as advertisements, as long as the identification is "clear and conspicuous." Although the Act does not define "clear and conspicuous," it does prohibit false or misleading header information and deceptive subject lines. 15 USC §7704(a)(1)-(2). E-mail headers, including "From," "To," and routing information such as the originating domain name and e-mail address, must accurately identify the sender. 15 USC §7704(a)(1).

© The Regents of the University of California

§17.16 (2) Notice and Opt-Out Mechanism

The CAN-SPAM Act has detailed requirements concerning opt-out procedures. Commercial e-mails must include a "clear and conspicuous notice" that the recipient has the option to refuse to receive future commercial e-mails from the sender. 15 USC §7704(a)(5). In addition, commercial e-mails must "clearly and conspicuously" display a functioning return e-mail address or other Internet-based mechanism that a recipient can use to submit an opt-out request. Technologically, the return e-mail address or other opt-out mechanism must remain capable of receiving opt-out requests for at least 30 days after the original e-mail was sent. (Temporary disruptions caused by technical problems outside the sender's control will not trigger violations of the Act if corrected within a reasonable time period.) 15 USC §7704(a)(3)(C). Senders may comply with the opt-out requirement by offering the recipient a menu of options regarding the types of e-mail that the recipient does or does not want to receive from the sender, as long as one of the options allows the recipient to choose not to receive any further commercial e-mail from the sender. 15 USC §7704(a)(3)(B). A recipient may not be required to pay a fee to opt out or provide any information other than his or her e-mail address and opt-out preferences; no steps may be required in the opt-out process other than sending a reply e-mail message or visiting a single page on an Internet website. 16 CFR §316.5.

Once a recipient makes an opt-out request, the sender must honor the request within 10 business days. It is unlawful for the sender (or anyone acting on behalf of the sender, such as an e-mail marketer) to send any commercial e-mails after the 10-business-day period to a recipient who has opted out. 15 USC §7704(a)(4)(A).

© The Regents of the University of California

§17.17 (3) Postal Address

The third content requirement for commercial e-mails is straightforward. All commercial e-mails must include a valid physical postal address, which may be the sender's current street address, an accurately registered Post Office box, or a private mailbox the sender has accurately registered with a commercial mail receiving agency established according to postal service regulations. 16 CFR §316.2(p).

© The Regents of the University of California

§17.18 (4) Affirmative Consent

"Affirmative consent" means that the recipient has expressly consented to receive the e-mail, either at the recipient's own initiative or in response to a clear and conspicuous request for consent. 15 USC §7702(1)(A). If an e-mail is to be transmitted by a party other than the party to whom the recipient gave consent, then the recipient must be given "clear and conspicuous notice at the time the consent was communicated" that his or her address could be transferred to such other party for initiation of commercial e-mail messages. 15 USC §7702(1)(B). As noted in §17.14, commercial e-mail messages need not be identified as advertisements if a recipient has given affirmative consent to their receipt. Further, if a recipient opts out of receiving e-mails, but later gives affirmative consent to receipt, the consent will override the opt-out request and allow commercial e-mails to be sent to that recipient. 15 USC §7704(a)(4)(B). Finally, the requirements for identification of sexually oriented e-mail messages (see §17.20) do not apply if a recipient has given affirmative consent to their receipt. 15 USC §7704(d)(2).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/17 Advertising on the Internet/§17.18A (5) Forwarding Commercial E-Mails

§17.18A (5) Forwarding Commercial E-Mails

In the Statement of Basis and Purpose issued with the final CAN-SPAM Act (16 CFR §§316.1-316.6), the FTC addressed commercial "forward to a friend" e-mails. See 73 Fed Reg 29654 (2008). When the recipient of a commercial e-mail forwards the message, the issue for CAN-SPAM compliance is whether the seller or the forwarder is the "sender" as defined in 16 CFR §316.2(m). A seller who induces the original recipient to forward the e-mail with offers of compensation or other consideration is likely to be considered the sender or initiator of the message, and therefore responsible for assuring that the message complies with CAN-SPAM.

© The Regents of the University of California

§17.19 d. Deceptive E-Mail Practices

The CAN-SPAM Act details a series of fraudulent and abusive e-mail practices that constitute violations of the Act. These include, among other things, using materially false header information, using false or misleading subject lines, registering for e-mail accounts under false names, falsely representing oneself to be the owner of multiple e-mail accounts and sending multiple e-mails from those accounts, and sending e-mails from a computer accessed without permission. 18 USC §1037; 15 USC §7704(a). The Act also prohibits so-called "dictionary attacks" (compiling e-mail addresses by automatic generation of random combinations of letters and numbers) and e-mail address "harvesting" (collecting e-mail addresses by automated means from websites or online services such as newsgroups, bulletin boards, or chat rooms), as well as the transmission of messages to any e-mail addresses that have been obtained in this way. 15 USC §7704(b).

The FTC has rule-making authority to specify additional activities or practices that will constitute violations of the Act if the FTC determines that these activities or practices are contributing to the proliferation of unlawful commercial e-mail. 15 USC §7704(c). The Department of Justice has the authority to seek criminal penalties for e-mailers that send commercial e-mail from a computer without authorization, falsify e-mail header information to hide the true origin of the message ("spoofing"), register for multiple e-mail accounts with false identification information, or falsely represent themselves as owners of multiple IP addresses used to send commercial e-mails. See http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus61.shtm.

© The Regents of the University of California

§17.20 e. Sexually Oriented Materials

The CAN-SPAM Act also requires that warning labels be placed on commercial e-mail containing sexually oriented materials. 15 USC §7704(d). Unless the recipient has affirmatively consented to receiving such e-mail (15 USC §7702(1)), anyone sending an e-mail message containing sexually oriented materials must exclude sexually oriented materials from the subject heading and include as the first 19 characters of the subject heading "SEXUALLY-EXPLICIT:" (in capital letters). 16 CFR §316.4(a)(1). When opened, the initially viewable portion of the message must also contain the "SEXUALLY-EXPLICIT:" phrase, as well as the following (16 CFR §316.4(a)(2)):

- Clear and conspicuous identification that the message is an advertisement or solicitation;
- Clear and conspicuous information on how to opt out of future messages;
- A functioning return e-mail address or similar Internet-based mechanism that the recipient can use to opt out of future messages, and that operates for at least 30 days after transmission of the message;
- A valid physical postal address of the sender; and
- Instructions on how to access, or a mechanism to access, the sexually oriented material.

The initial message cannot contain any sexually oriented material, but only instructions on how to access the material. 15 USC §7704(d)(1)(B). Violations of these requirements are subject to criminal penalties, including fines or imprisonment of not more than 5 years. 15 USC §7704(d)(5).

© The Regents of the University of California

§17.21 f. Attribution Rules

The CAN-SPAM Act includes an attribution rule holding companies responsible for violations by other parties, such as e-mail marketers, in e-mail promotions of the company's products or services, if the company knew or should have known of the promotion and took no steps to prevent it. See 15 USC §7705. As a result, a company will not escape the Act's reach simply by hiring an outside firm to send e-mail advertisements on its behalf. See *U.S. v Cyberheat, Inc.* (D Ariz, Mar. 2, 2007, No. CV 05-457-TUC-DCB) 2007 US Dist Lexis 15448 (company liable for CAN-SPAM violations of its affiliates). If a company operates through several divisions or lines of business, but only one division holds itself out to an e-mail recipient as the sender, then only that division is treated as the sender for purposes of the Act. 15 USC §7702(16)(B).

© The Regents of the University of California

§17.22 g. Enforcement of CAN-SPAM

The Federal Trade Commission (FTC) (along with the U.S. Department of Justice) has primary responsibility for administering and enforcing the CAN-SPAM Act. Violations of the Act are subject to criminal penalties and, in addition, are treated as unfair or deceptive trade practices under the FTC Act. 15 USC §57a(a)(1)(B). See §§17.4-17.7. The FTC has the same jurisdiction, powers, and duties with respect to enforcement of the CAN-SPAM Act as it has under the FTC Act. 15 USC §§41-77. See 15 USC §7706. Significantly—and unlike the California anti-spam law—the CAN-SPAM Act does not give individual spam recipients the right to sue spammers for damages or injunctive relief. State attorneys general, as parens patriae on behalf of state residents, and Internet service providers (ISPs) have limited rights to bring civil suits to enforce the Act. See 15 USC §7706. In addition to injunctive relief, state attorneys general may seek statutory damages of $250 per unlawful message, up to a maximum of $2 million (15 USC §7706(f)), and ISPs can sue for up to $100 per unlawful message, up to a maximum of $1,000,000 (15 USC §7706(g)). For purposes of the ISP right of action, courts have given broad construction to the CAN-SPAM phrase "provider of Internet access service," so that the enforcement right is available not only to large commercial ISPs but also to smaller providers of online services, even if those providers do not offer the full range of services sold to subscribers by large commercial ISPs. See *Hypertouch, Inc. v Kennedy-W. Univ.* (ND Cal, Mar. 8, 2006, No. C04-05203 SI) 2006 US Dist Lexis 14673 (defining "Internet access service" for purposes of CAN-SPAM).

Following are selected FTC enforcement actions under CAN-SPAM:

- A network of companies and individuals was charged under the CAN-SPAM Act with failing to include the required "SEXUALLY-EXPLICIT" labeling and using false and misleading transmission information, deceptive subject headings, and nonfunctioning opt-out mechanisms to sell and provide access to pornography online. Defendants paid $621,000 to settle the charges and had agreed to ongoing monitoring. See *FTC v Global Net Solutions, Inc.* (D Nev 2005) Civ Action No. CV-S-05-0002-PMP-LRL. Case-related documents are available at http://www.ftc.gov/os/caselist/0423168/0423168.shtm.
- Unwanted e-mail messages that misrepresented hoodia weight-loss products and human growth hormone anti-aging products and failure to provide clear and conspicuous notice to opt out of future e-mails from the sender resulted in a judgment of $2.5 million for the FTC. See *FTC v Sili Neutraceuticals, LLC* (ND Ill 2007) Civ Action No. 07C 4541. Case-related documents are available at http://www.ftc.gov/os/caselist/0723124/index.shtm.
- Online advertiser ValueClick was fined $2.9 million for falsely advertising "free" gifts to consumers to lure them to websites and failing to fulfill its promise to secure consumer financial information. The settlement required ValueClick to conspicuously disclose the actual costs to consumers of the "free" gifts." See *U.S. v ValueClick, Inc.* (CD Cal 2008) Case No. CV08-01711 MMM (RZx). Case-related documents are available at http://www.ftc.gov/os/caselist/0723111/index.shtm.
- Following issuance of a permanent injunction in 2006 to prevent further "phishing," "pagejacking," and "mousetrapping" activities by the defendants, the FTC in 2008 sought a civil contempt order requiring defendants to disgorge profits from those activities, which included modifying or replacing the functions of users' web browsers and collecting users' personally identifiable information without the users' "prior, express consent." See *FTC v Odysseus Mktg., Inc.* (D NH 2005) Civ Case No. 05-CV-330 SM. Case-related materials are available at http://www.ftc.gov/os/caselist/0423205/0423205.shtm.

In *MySpace, Inc. v Wallace* (CD Cal 2007) 498 F Supp 2d 1293, in a default judgment, Internet access provider MySpace was awarded $230 million for CAN-SPAM violations, $4.5 million in attorney fees, and an additional $1.5 million for defendants' violations of California's anti-phishing statute as a result of the defendants' multifaceted scheme to disseminate commercial messages to MySpace users. The defendants used an automated bot program to create over 11,000 MySpace profiles from which they sent messages and posted comments intended to redirect other MySpace users to a website designed to hijack login information by depicting the MySpace logo and a username and password prompt. In total, 400,000 messages were sent and 890,000 comments were posted from 320,000 hijacked accounts.

© The Regents of the University of California

§17.23 h. National "Do Not E-Mail" Registry

CAN-SPAM set in motion the establishment of a national "Do Not E-Mail" registry, similar to the existing "Do Not Call" registry implemented by the FTC, the FCC, and state governments. See http://www.ftc.gov/donotcall. Under CAN-SPAM, the FTC had 6 months in which to establish a plan and timetable for establishing a "Do Not E-Mail" registry and to identify any technical, practical, privacy-related, or enforceability-related concerns that the FTC has in connection with the registry. The Act then authorized the FTC to implement the registry no earlier than 9 months after the date of enactment of the Act. See 15 USC §7708.

In June 2004, the FTC issued a report concluding that a national "Do Not Email" registry would fail to reduce the amount of spam that consumers receive, and could even increase it. The text of the report is available at http://www.ftc.gov/reports/dneregistry/report.pdf. The FTC assessed various options for an effective registry and concluded that none could be enforced adequately. Instead, the FTC recognized the need for an e-mail authentication standard and concluded that anti-spam efforts should, for now, focus on creating a robust system that would prevent spammers from hiding their tracks as well as law enforcement and anti-spam filters. See *New System to Verify Origins of E-Mail Must Emerge Before "Do Not Spam" List Can Be Implemented, FTC Tells Congress* (June 15, 2004), at http://www.ftc.gov/opa/2004/06/canspam2.htm.

© The Regents of the University of California

§17.23A i. Commercial E-Mails Sent to Wireless Devices

Under the CAN-SPAM Act, the FCC, in conjunction with the FTC, promulgated rules to protect consumers from unwanted mobile service commercial messages (MSCMs). See 15 USC §7712(b). The regulations provide protection against unwanted commercial messages sent to wireless devices, telephone solicitations made to wireless numbers registered on the national Do-Not-Call List, and autodialed text messages. See 47 CFR §64.3100. Note that the regulations cover only commercial messages that are sent using an Internet address that includes an Internet domain name (*e.g.,* mailto:sender@domainname.com). The regulations apply to advertisements but not to "transactional or relationship" messages, such as account updates or warranty information. 47 CFR §64.3100(c)(2), (c)(8). See §17.13.

The FCC regulations, designed to ban unwanted advertisements from cell phones, pagers, or PDAs, do not apply to e-mail forwarded from a computer to a wireless device, noncommercial messages, or "short messages" sent without an Internet address, such as mobile phone text messages. See http://www.fcc.gov/cgb/consumerfacts/canspam.html.

Express prior authorization from a recipient must be obtained before using the Internet to send an advertisement to a wireless device. 47 CFR §64.3100(a)(1). All subsequent authorized commercial electronic messages must clearly and conspicuously display a functional e-mail address to receive requests to revoke authorization or opt out of receiving future messages. 47 CFR §64.3100(b)(2). The e-mail display must be accessible without requiring the subscriber to view additional commercial content. Senders of MSCMs must also disclose their name in the message and provide at least one cost-free method of opting out of future advertisements. 47 CFR §64.3100(b)(4)-(5). In addition, anyone sending an MSCM must provide a clear option to reject future messages by the same electronic medium that was used to opt in. 47 CFR §64.3100(b)(3). Senders have 10 days to comply with opt-out requests. 47 CFR §64.3100(b)(1).

To assist the FCC, all wireless service providers are required to submit the Internet domain names used to transmit e-mails to wireless devices. 47 CFR §64.3100(e). Marketers may not send commercial e-mail to the listed domain names without the recipient's express prior authorization. For more information, see http://www.fcc.gov/cgb/consumerfacts/canspam.html. The domain names list is available at http://www.fcc.gov/cgb/policy/DomainNameDownload.html. Senders have 30 days from the posting of a new domain name on the list to cease transmitting messages to any Internet address containing the domain name. 47 CFR §64.3100(a)(4).

The FCC may enforce FTC requirements for commercial messages sent to nonwireless devices, including desktop computers, in situations when the sender is a communications company or the advertisement promotes a product of such a company. See http://www.fcc.gov/cgb/consumerfacts/canspam.html.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/17 Advertising on the Internet/§17.23B j. Criminal Liability Under CAN-SPAM

§17.23B j. Criminal Liability Under CAN-SPAM

CAN-SPAM also includes provisions establishing criminal liability for fraud and related activity in connection with e-mail. The following are criminal acts under 18 USC §1037(a):

- Accessing a protected computer without authorization and intentionally initiating multiple commercial e-mails from or through that computer;
- Using a protected computer to relay multiple commercial e-mails with the intent to deceive or mislead recipients, or any Internet service provider, regarding the origin of those e-mails;
- Including materially false header information in multiple commercial e-mails and intentionally initiating their transmission;
- Registering 5 or more e-mail or online user accounts or 2 or more domain names using material false information regarding the identity of the registrant, and intentionally initiating the transmission of multiple commercial e-mails from any combination of those accounts or domain names; and
- Falsely representing oneself to be the registrant (or the legitimate successor in interest to the registrant) of 5 or more Internet addresses and intentionally initiating the transmission of multiple commercial e-mails from such addresses, or conspiring to do so.

The term "multiple" is defined as more than 100 e-mail messages during a 24-hour period, more than 1000 during a 30-day period, or more than 10,000 during a 1-year period. 18 USC §1037(d)(3).

These acts may be punishable by fines, imprisonment for up to 5 years, or both, depending on the circumstances. See 18 USC §1037(b). The defendant may also be ordered to forfeit real or personal property traceable to the offense. See 18 USC §1037(c).

© The Regents of the University of California

2. State Anti-Spam Laws

§17.24 a. Generally

Before the enactment of CAN-SPAM, California had its own anti-spam legislation. See Bus & P C §§17529-17529.9, 17538.45. And California was not alone. At least 34 states have had anti-spam legislation, including Missouri (RS Mo 407.1123), Nevada (NRS 41.730), Arizona (ARS 44-1372), Arkansas (ACA 4-88-603), New Mexico (NM Stat 57-12-23), Oklahoma (15 Okla St 776.1), Maryland (Md Comm C 14-3002), West Virginia (W Va C 46A-6G-1—46A-6G-5), Maine (Me Rev Stat Ann tit. 10 §1497), Illinois (815 ILCS 511/10), Pennsylvania (18 Pa CS 7661), Tennessee (Tenn Code 47-18-2501), and Rhode Island (RI Gen Laws 11-52-4.1). For a summary of state anti-spam laws as of mid-2003, see http://www.the-dma.org/antispam/statespamlaws.shtml. The laws of several states impose much tougher requirements than the CAN-SPAM Act, *e.g.,* by mandating an opt-in, rather than an opt-out, regime, by requiring specific labeling ("ADV" or the like) in the subject line, and by creating a private right of action for spam recipients. See §17.26 for discussion of the scope of CAN-SPAM's preemption of state law.

© The Regents of the University of California

§17.25 b. California Anti-Spam Laws

The centerpiece of California's anti-spam law, Bus & P C §17529.2 (also referred to as SB 186 (2003)), was an outright prohibition on all unsolicited commercial e-mail sent from California or to a California e-mail address, unless the recipient had consented to receive it or the recipient had a "preexisting or current business relationship" with the sender. See Bus & P C §17529.1(o). This provision has clearly been preempted by the CAN-SPAM Act. See §17.26.

Another section of California's anti-spam law, Bus & P C §17529.4(a), prohibits any person or entity from collecting e-mail addresses posted on the Internet for the purpose of initiating, or advertising in, unsolicited commercial e-mail advertisements sent from California or to a California e-mail address. The California anti-spam law also prohibits a number of questionable or fraudulent business practices, including compilation of e-mail addresses by automated means (Bus & P C §17529.4(b)), use of a third party's domain name without permission (Bus & P C §17529.5(a)(1)), use of "falsified, misrepresented, or forged" information in e-mail headers (Bus & P C §17529.5(a)(2)), and knowing use of a materially misleading subject line (Bus & P C §17529.5(a)(3)). As discussed in §17.26, these provisions have probably not been preempted by CAN-SPAM.

The California anti-spam law creates a right of civil action, on the part of spam recipients, e-mail service providers, and the state attorney general, against violators for recovery of both actual damages and liquidated damages of $1000 per unsolicited commercial e-mail advertisement, up to $1 million per incident, together with reasonable attorney fees and costs if the plaintiff prevails. Bus & P C §§17529.5, 17529.8. As discussed in §17.26, this private right of action may have survived as a civil remedy against deceptive or fraudulent e-mail practices, but has probably not survived otherwise.

California's anti-spam law also includes a prohibition against use of an e-mail service provider's equipment to deliver unsolicited e-mail advertisements to registered users of the service in violation of an anti-spam policy of that service provider (Bus & P C §17538.45(c)):

> No individual, corporation, or other entity shall use or cause to be used, by initiating an unsolicited electronic mail advertisement, an electronic mail service provider's equipment located in this state in violation of that electronic mail service provider's policy prohibiting or restricting the use of its equipment to deliver unsolicited electronic mail advertisements to its registered users.

An e-mail service provider has the right to sue for violations of its policy and to recover the greater of actual monetary loss or liquidated damages of $50 per e-mail up to a maximum of $25,000 per day, plus reasonable attorney fees. Bus & P C §17538.45(f). The extent to which these provisions have been preempted by CAN-SPAM is uncertain.

A violation of Bus & P C §17529.5 is a misdemeanor punishable by a fine of up to $1000, up to 6 months in prison, or both.

© The Regents of the University of California

§17.26 c. Scope of Preemption of California Law by CAN-SPAM Act

Section 8(b)(1) of the CAN-SPAM Act (15 USC §7707(b)(1)) provides that the Act "supersedes any statute, regulation, or rule of a State … that expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic message or information attached thereto." This section effectively preempts the core operative provision of California's anti-spam law, namely, Bus & P C §17529.2, which imposed a blanket prohibition on all unsolicited commercial e-mail unless the recipient consented to receive it or there was a preexisting or current business relationship between sender and recipient. Bus & P C §§17529.1(o), 17529.2. See §17.24.

There remain areas of uncertainty, however, regarding the scope of federal preemption. For example, Bus & P C §17529.5 prohibits the use of a third party's domain name without authorization, false e-mail header information, and misleading subject lines. In general, §17529.5 should fall within the exception to preemption in 15 USC §7707(b)(1) for state laws prohibiting false or deceptive e-mails, and thus should remain in effect. However, Bus & P C §17529.4, which prohibits certain questionable e-mail practices such as compiling e-mail addresses by automated means or using programs to create multiple e-mail accounts used for sending spam, has been ruled preempted by the CAN-SPAM Act. In *Facebook, Inc. v ConnectU LLC* (ND Cal 2007) 489 F Supp 2d 1087, 1094, the court held that §17529.4 does not attempt to regulate false or deceptive e-mail and therefore does not fall within the exception to preemption in 15 USC §7707(b)(1) for state laws prohibiting false or deceptive e-mails.

Although much of the California anti-spam law is preempted by CAN-SPAM, violations that are not preempted are subject to fines of up to $1000 per unwanted commercial message, up to $1 million per incident. Bus & P C §17529.5. The overlapping uncertainties between state anti-spam legislation and CAN-SPAM can be resolved only by further congressional action or on a case-by-case basis in the courts.

The CAN-SPAM Act does not preempt state laws that are not specific to e-mail, such as state trespass, tort, and contract laws and state laws relating to fraud or computer crime. 15 USC §7707(b)(2). Further, the Act does not attempt to prohibit or otherwise regulate the adoption or enforcement of any policy by an ISP declining to transmit or store certain types of e-mail messages. 15 USC §7707(c). Thus, companies with e-mail advertising programs will remain subject to any anti-spam policies of an ISP, although the California statute (Bus & P C §17538.45) that made violation of an ISP's anti-spam policy also a violation of California law may have been preempted by the CAN-SPAM Act.

Although CAN-SPAM has been praised by e-mail marketers for creating a national standard, it has also been criticized for being too lenient. Critics of the Act's broad preemptive provisions include the National Association of Attorneys General; see Kuchinskas, *AGs Want to Can the Can Spam Bill*, Internetnews.com (Nov. 6, 2003), available at http://www.clickz.com/showPage.html?page=3105361. Addressing these complaints will require either additional federal legislation or carefully drafted state legislation designed to exist in the few gaps left open by CAN-SPAM.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/17 Advertising on the Internet/§17.27 d. Penal Code §502(c)

§17.27 d. Penal Code §502(c)

Penal Code §502(c) establishes criminal penalties for a variety of computer-related offenses. As noted in §17.26, the CAN-SPAM Act does not preempt state laws relating to fraud or computer crime. Section 502(c) therefore continues in force in California. Although most of the offenses listed in §502(c) are broadly directed at hacking and service disruptions (see chap 18), Pen C §502(c)(3) prohibits knowing use of computer services without permission, and Pen C §502(c)(9) prohibits knowing and unpermitted use of "the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more e-mail messages, and thereby damages or causes damage to a computer, computer system or computer network." Both of these statutes may be implicated in spam. Violations are punishable by fines that in certain cases may range up to $10,000 or by imprisonment or both. See Pen C §502(d)(2), (5). In addition, any owner or lessee of a computer, computer system, computer network, computer program, or data who suffers damage or loss because of a violation of Pen C §502(c) may bring a civil action for compensatory damages and injunctive or other equitable relief under Pen C §502(e)(1), as well as any relief available under other applicable law.

© The Regents of the University of California

§17.28 3. Anti-Spam Litigation

Plaintiffs have been increasingly successful in bringing civil actions against spammers on various legal grounds. For example, in *EarthLink, Inc. v Carmack* (ND Ga, May 7, 2003, No. 1:02-CV-3041-TWT) 2003 US Dist Lexis 9963, the federal district court entered judgment of $16.4 million, including punitive damages and attorney fees, for EarthLink, an internet service provider. The court found that the defendant sent more than 825 million unsolicited commercial e-mails to EarthLink subscribers, and held that his spamming and "spoofing" (obscuring the true source of his e-mails by using false headers) violated federal and state RICO laws.

The potential bases for civil actions against spammers vary, and courts are increasingly willing to entertain different theories of recovery. In *CompuServe, Inc. v Cyber Promotions, Inc*. (SD Ohio 1997) 962 F Supp 1015, the court found that the defendant's spamming of the plaintiff's customers constituted a trespass to chattels, which caused actual damage to the plaintiff when its subscribers terminated their accounts as a result of the defendant's actions. 962 F Supp at 1023. The court rejected the defendant's First Amendment defense. 962 F Supp at 1027. For further discussion of the tort of trespass to chattels in Internet-related litigation, see §§18.17-18.21.

In *America Online, Inc. v National Health Care Discount, Inc.* (ND Iowa 2001) 174 F Supp 2d 890, the court upheld AOL's claim of trespass to chattels against a spammer and also allowed AOL's claim under the Computer Fraud and Abuse Act (18 USC §1030). Although the Computer Fraud and Abuse Act is primarily a criminal statute, it also creates a private right of action for compensatory damages and injunctive relief (see 18 USC §1030(g)) for (18 USC §1030(a)-(c)):

> knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer; [or] intentionally access[ing] a protected computer without authorization, and as a result of such conduct, recklessly caus[ing] damage.

The court found that the defendant's e-mails "intentionally accessed AOL's computers, and intentionally caused the transmission of information" (174 F Supp 2d at 899), and that the volume of unsolicited e-mails had created a substantial burden on AOL's computer system.

In *Cyber Promotions, Inc. v America Online, Inc.* (ED Pa 1996) 948 F Supp 436, a spammer who had failed to persuade the court that its spamming activities were protected by the First Amendment asserted an antitrust claim against AOL for blocking its unsolicited e-mails. The court rejected the claim, noting that the plaintiff and AOL were not competitors, and that even if they were, it was unlikely that AOL monopolized the plaintiff's advertising capabilities by supplying AOL subscribers with a means of blocking the plaintiff's unsolicited e-mail.

© The Regents of the University of California

§17.29 4. Practical Methods of Blocking Spam E-Mail

While legislative efforts against spam progress, the FTC, state agencies, and ISPs are beginning to promote user-based ways to limit the amount of spam. ISPs now typically offer services such as spam filters, sometimes implementing them automatically and offering subscribers guidance on how to maximize their effectiveness. In addition, the FTC suggests several practical, low-cost methods of avoiding spam e-mail (see http://www.ftc.gov/spam), including the following:

- Taking steps to "mask" an e-mail address. E-mail addresses can be masked so that they are not collected by "spiders" (automated programs used by spammers to harvest e-mail addresses they find on websites). For example, rather than displaying an e-mail address as "jdoe@lawfirm.com," a newsgroup or message board posting could display the address as "jdoe at lawfirm.com" or "jdoe at lawfirm dot com." The FTC suggests that inserting an additional word (one that is obviously included to deter spam, such as "NOSPAM") into displayed e-mail addresses can have the same result, so that by displaying an e-mail address as "jdoe@NOSPAM.lawfirm.com," spiders would not collect a valid e-mail address, while human users would know to remove the word "NOSPAM" before sending an e-mail.
- Using a screen name that is not associated with your e-mail address when using a chat room.
- Using unique e-mail addresses so that spammers who use "dictionary attacks" to e-mail various name combinations cannot detect your e-mail address.
- Setting up two e-mail accounts, so that spam can be forwarded to a second account and later be disposed of.

The FTC has also suggested changing the settings of e-mail servers to reduce spam. See http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus57.pdf. Mail servers usually maintain an open door (an "open relay") to the Internet, which can be accessed and used for spamming. When an e-mail message is sent from a secure server, the software checks to see if the sender is listed as a user within the organization. If the sender is confirmed as a user, the e-mail is sent. According to the FTC, if the server is not secure, and it contains an open relay, the mail server can be configured to accept and transfer e-mail on behalf of anyone (including outside third parties).

Reporting spam to the FTC at spam@uce.gov may cause the FTC to initiate an investigation if it appears that the spammer has violated the FTC Act. Users might also consider reporting the spam to the sender's ISP. Some ISPs provide their subscribers with free programs to block e-mail from senders known to disseminate junk e-mail.

The website of the California Department of Consumer Affairs, Office of Privacy Protection, at http://www.privacy.ca.gov, contains links to sites offering practical information on how to block spam.

© The Regents of the University of California

E. Search Engine Optimization

§17.29A 1. Overview

Search engine optimization (SEO) is the process of creating and modifying a website to increase the likelihood that the site will appear at or near the top of the search results produced by leading search engines. See Lanz, Using the Internet to Attract Clients, http://www.calbar.ca.gov/state/calbar/calbar_cbj.jsp?sCategoryPath=/Home/Attorney%20Resources/California%20Bar%20Journal/April2008&MONTH=4&YEAR=2008&sCatHtmlTitle=MCLE%20Self-Study&sJournalCategory=YES.

Successful SEO tactics improve profits by increasing website visitors and client bases, but care must be taken to comply with Internet service provider (ISP) policies and contractual restrictions, as well as the policies of the search engines themselves. For example, some methods that can be used to optimize a site for these purposes may be viewed by the ISP or search engine as spam violations. See, *e.g.*, Google's webmaster guidelines at http://www.google.com/support/webmasters/bin/answer.py?answer=35769. As discussed in §3.71, trademark law may also be implicated.

© The Regents of the University of California

§17.29B 2. Optimization Tools and Techniques

The core of SEO is the modification of a website to improve its quality and organization. SEO tools include keyword selection and display, quality link building, updating quality content, and website tuning. Counsel should watch for the following practices in a review of a client's SEO activities or an agreement with an SEO consultant.

The client should be counseled to avoid methods that violate search engine policies, otherwise known as "black hat" methods. In any website review conducted for clients, counsel should consider carefully the methods used in search engine optimization to confirm that they are appropriate and do not create unacceptable risk.

Some black hat methods use tools to create optimized websites intended for nonhuman viewers. One tool used for this purpose is the "doorway page." Programmed to be visible only to search engine spiders, doorway pages are copies of "real" pages altered to be filled with selected keywords and to promptly redirect live users to the "real" website. See http://www.google.com/support/webmasters/bin/answer.py?answer=66355. Google considers this spam and penalizes this activity by de-ranking or removing a website from the search index. See, *e.g.*, "Google Imposes a Ban on BMW Web Site" at http://www.nytimes.com/2006/02/07/technology/07bmw.html?_r=2&oref=slogin&oref=slogin.

Another black hat tool is automated page creation, where multiple websites are created based on templates that effectively spam search engines and artificially increase rankings. This technique is also known as spamdexing. See Nathenson, *Internet Infoglut and Invisible Ink: Spamdexing Search Engines with Meta Tags*, 12 Harv J Law & Technol 43 (1998). These practices also violate search engine policies.

"Cloaking," or serving different pages to website visitors depending on certain criteria (for example, whether the viewer is a real end user or an automated web indexer used by a search engine company), is another black hat tactic. http://www.google.com/support/webmasters/bin/answer.py?answer=66355. Programs on the server side analyze fields such as IP address, user-agent http header, http_referrer header, and http accept-language header, and then display the alternate page to the visitor. Once they become aware of the use of this technique, search engines generally respond by removing cloaked pages and their domain names from search indexes. http://www.google.com/support/webmasters/bin/answer.py?answer=66355.

The most sinister practitioners of black hat techniques illicitly attack competitors' websites to lower rankings. See http://www.forbes.com/2007/06/28/negative-search-google-tech-ebiz-cx_ag_0628seo.html. Often referred to as "googlebowling," these tools include so-called ping spam, referral spam, blog spam, e-mail spam, fake domain spam, and link-killing, and may be used, *e.g.,* to create links to the site from other sites that are already banned from a search index.

Although many SEO practices violate search engine policies, the goal of increasing the quality of search results may still be accomplished by adhering to those policies. Most search engines post guidelines and tips for increasing the quality of website material and maximizing search engine results. See, *e.g.,* http://www.google.com/support/webmasters/bin/answer.py?answer=35769; http://help.yahoo.com/l/us/yahoo/search/ranking/ranking-02.html. The legal status of certain SEO tactics remains questionable. See Grimmelmann, *The Structure of Search Engine Law*, 93 Iowa L Rev 1 (Nov. 2007).

© The Regents of the University of California

II. INTERNET ADVERTISING AGREEMENTS

§17.30 A. Overview

Advertising on the Internet differs from advertising in conventional media in several respects. The Internet's ability to take advantage of multimedia and utilize audio and video as well as text and graphics has resulted in new forms of advertising. These include "advertainment," *i.e.,* animated or live action short film subjects that are streamed to viewers as content but that also promote a product or a service, and 3-D visualizations, which permit a potential buyer to view a product in a three-dimensional manner from different angles or to manipulate an object virtually in order to inspect its functional or decorative aspects as if the user held the product in hand. Sections 17.31-17.36 discuss the structure and content of several types of agreements for Internet-based advertising, including banner ads, Internet business directory advertising, and portal-based advertising.

© The Regents of the University of California

§17.31 B. Banner Advertising

Banner advertisements are text and graphic images that appear on a website page (often at the top) when a website user views the page content. Like an interactive billboard, a banner ad provides information concerning the advertiser's products or services and also permits the user to "click through" the ad to obtain more information or to make selections. Banner advertising is often priced by measuring the frequency with which the banner appears and click-through percentages (the percentage of viewers of the web page who click on the banner ad to obtain further information). The cost is often measured in "cost per thousand" (CPM)—the amount of money paid per thousand banners served (also known as "impressions") at a website. Advertisers determine the demographics they wish to target, match those demographics to a particular website or group of websites, and negotiate with the advertising representatives of the host websites for placement of the ad. The host site will "serve" or post the banner ads and provide reporting on click-throughs.

One key issue for negotiation is how frequently the advertiser's banner will be displayed on the host website. The advertiser may end up sharing its banner location with other advertisers (with the ads changing every few minutes) unless the advertiser purchases all impressions available on the host website.

The sample agreement in §17.32 is intended for use when contracting with a website sponsor to host banner ads.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/17 Advertising on the Internet/§17.32 C. Form: Banner Advertising Agreement

§17.32 C. Form: Banner Advertising Agreement

To download **Word** version, right click and choose *Save Target As*

To download **WordPerfect** version, right click and choose *Save Target As*

BANNER ADVERTISING AGREEMENT

This BANNER ADVERTISING AGREEMENT (this "Agreement") is entered into as of _ _[*date*]_ _ between _ _[*purchaser*]_ _ ("Advertiser") and _ _[*provider*]_ _ ("Company").

WHEREAS, Advertiser operates a commercial Internet website and desires to advertise its goods or services on the Internet; and

WHEREAS, Company desires to provide to Advertiser, and Advertiser desires to obtain from Company, advertising services in the form of banner ad placement on Company's Internet website located at _ _[*website address*]_ _ (the "Site").

NOW THEREFORE, in consideration of the mutual promises contained herein, the parties agree as follows:

1. SERVICES.

(a) Company agrees to perform the following services on a nonexclusive basis: storage, presentation, copying, transmission, performance, and display of all graphical image files, text, animation, software, Internet links, and trademarks provided by Advertiser to Company and described on Exhibit A to this Agreement (the "Banner") on and through Company's Site and available to persons accessing Company's Site via the Internet ("Users").

(b) Company shall provide Advertiser with written reports on a monthly basis setting forth the total number of impressions, pages, or instances in which the Banner is accessed by users via the Internet and other reports as specified in Exhibit A.

Comment: The website host's reporting obligation under this agreement should reflect all of the data that the advertiser needs to evaluate the success of the program. Measuring impressions may be useful, but it may also be helpful to know from which web page a user clicked through or what demographics, if any, the host company has on the users accessing the site during the reporting period.

(c) The timing and frequency of Banner display shall be as set forth in Exhibit A. Advertiser understands that there is no guarantee that the Banner will be displayed as scheduled and understands that the operability and accessibility of the Banner may be limited by (1) equipment failure, (2) periodic maintenance, and (3) causes beyond the Agency's control such as interruption of telecommunications transmissions, viruses, network congestion, and other failures.

Comment: Advertisers can also specify the location of the banner ad, including both its location on the page and its location within the structure of the host company's website, *i.e.,* on the home page or on all pages.

2. LICENSE. Advertiser grants to Company a nontransferable, nonexclusive, worldwide license during the term of this Agreement, solely for the purpose of performing this Agreement, to (a) copy, store, use, publicly display, publicly perform, and transmit the Banner; and (b) display Advertiser's trademarks and logos contained in the Banner. Such rights may be sublicensed to other Internet sites solely for the limited purpose of dissemination of the Banner and performance of this Agreement.

3. PROPRIETARY RIGHTS. Advertiser retains all rights, title, and interest in the Banner and Advertiser's trademarks and logos, derivative works, modifications, and enhancements to the Banner developed by Advertiser or Company. Company retains all interest in the Site and any intellectual property contained therein, except the rights retained by Advertiser hereunder.

4. SECURITY. Company will implement and maintain commercially reasonable security measures to prevent the unauthorized use of the Banner and to ensure its integrity, including but not limited to (a) firewall protection, (b) data backup systems and procedures, and (c) virus screening. Company does not guarantee, however, that the Site will be error free or available on an uninterrupted basis.

5. CONTENT RESTRICTIONS. Company reserves the right in its discretion to refuse to perform this Agreement with respect to any version of the Banner that (a) fails to conform to Company's technical standards set forth on Exhibit B (subject to change on 30 days' notice to Advertiser); (b) actually or in Company's determination potentially violates any applicable law or infringes the intellectual property rights of third parties; (c) contains any images, text, or other content that in Company's determination is abusive, obscene, pornographic, defamatory, harassing, offensive, threatening, or malicious.

6. FEES. Fees for the services rendered hereunder and applicable payment terms are as set forth in Exhibit A. Advertiser shall be responsible for and shall pay all sales, use, service, or other taxes with respect to the services provided hereunder, including interest and penalties, whether or not such taxes are reflected in Company invoices.

7. ADVERTISER WARRANTIES. Advertiser warrants to Company that (a) Advertiser has the right and authority to enter into and perform this Agreement; (b) the Banner conforms substantially to Exhibit A; (c) the Banner does not violate any of the content restrictions contained herein or the Company's technical standards; and (d) Advertiser owns the Banner and all intellectual property rights therein.

8. DISCLAIMER. OTHER THAN AS SPECIFICALLY SET FORTH HEREIN, THE SERVICES TO BE PROVIDED BY COMPANY ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. COMPANY DOES NOT WARRANT THAT ITS SERVICE OR THE SITE WILL BE UNINTERRUPTED OR ERROR FREE. COMPANY DOES NOT WARRANT THE RESULTS THAT MAY BE OBTAINED BY USING ITS SERVICES OR PLACING THE BANNER ON THE SITE.

9. LIMITATION OF LIABILITY. EXCLUSIVE OF ANY INDEMNIFICATION OBLIGATIONS HEREUNDER, IN NO EVENT SHALL COMPANY BE LIABLE TO ADVERTISER FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES WITH RESPECT TO ANY MATTER ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT EVEN IF COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. COMPANY'S TOTAL LIABILITY FOR DIRECT DAMAGES UNDER THIS AGREEMENT SHALL NOT EXCEED THE TOTAL FEES PAID BY ADVERTISER TO COMPANY HEREUNDER.

10. INDEMNIFICATION.

(a) BY ADVERTISER. Advertiser agrees to indemnify, hold harmless, and defend Company and its directors, officers, employees, and agents from and against any action, claim, demand, dispute, or liability, including reasonable attorney fees, arising from or relating to: (1) any allegation that the Banner infringes a third person's copyright, trademark or service mark, name, or trade name, or misappropriates a third person's trade secret, name, likeness, or identity; (2) any negligence or willful misconduct of Advertiser; (3) any allegation that the Banner is or causes a violation of law or constitutes false advertising or unfair competition under the law of any jurisdiction; and (4) any sale or license of Advertiser's goods or services to a third person from or relating to the Site or Banner. Advertiser agrees that Company shall have the right to participate in the defense of any such claim through counsel of its own choosing.

(b) BY COMPANY. Company agrees to indemnify, hold harmless, and defend Advertiser and its directors, officers, employees, and agents from and against any action, claim, demand, dispute, or liability, including reasonable attorney fees, arising from or relating to any gross negligence or willful misconduct of Company.

11. TERM AND TERMINATION

(a) TERM. The term of this Agreement shall commence on the Effective Date and shall continue for 12 months, unless terminated sooner as provided herein. The term of this Agreement shall automatically renew for successive 12-month terms unless either party provides written notice of termination to the other party at least 90 days prior to the expiration of such term of its desire not to renew.

(b) TERMINATION. This Agreement may be terminated: (1) immediately by either party by written notice in the event of a material breach of this Agreement by the other party that remains uncured for a period of 30 days after receipt of written notice thereof; (2) immediately by either party by written notice in the event a party makes a general assignment for the benefit of creditors, files a voluntary petition in bankruptcy or for reorganization or arrangement under the bankruptcy laws, if a petition in bankruptcy is filed against such party, or if a receiver or trustee is appointed for all or any part of the property or assets of such party; (3) by Company, immediately upon written notice to Advertiser; or (4) by a written agreement of the parties.

Comment: Under this provision, the company hosting the banner ad can terminate the agreement immediately on written notice. Such a clause provides ultimate flexibility for the host company, enabling it to swap banner advertisers or increase its rates at any time. This clause may be too onerous on the advertiser, however, and should be considered in light of the parties' circumstances and respective leverage. It would be preferable for the advertiser to receive a guaranteed rate for a minimum period of time.

(c) RETURN AND DESTRUCTION. On any termination or expiration of this Agreement, Company shall deliver to Advertiser all copies of the Banner in Company's possession, custody, or control and erase and remove all copies of the Banner from any computer equipment and media in Company's possession, custody, or control; provided, however, that Company may retain one copy of the Banner for archival purposes only.

(d) PAYMENT ON TERMINATION. In the event this Agreement is terminated, Advertiser shall pay Company for all Services undertaken in performance of its obligations hereunder up to the date of termination. Such payment is due and payable immediately upon receipt of the Company's invoice.

(e) SURVIVAL. The provisions of Sections 3, 6, 7, 8, 9, 10, 11, and 13 will survive the expiration or earlier termination of this Agreement.

13. MISCELLANEOUS

(a) INDEPENDENT CONTRACTORS. The parties and their respective personnel are and shall be independent contractors, and neither party by virtue of this Agreement shall have any right, power, or authority to act or create any obligation, express or implied, on behalf of the other party.

(b) ASSIGNMENT. Neither party may assign its rights, duties, or obligations under this Agreement to any person or entity, in whole or in part, without the prior written consent of the other party, such consent not to be unreasonably withheld.

(c) WAIVER. No waiver of any provision hereof or of any right or remedy hereunder shall be effective unless in writing and signed by the party against whom such waiver is sought to be enforced.

(d) SEVERABILITY. If any provision of this Agreement is determined by a court of competent jurisdiction to be invalid under any applicable law, the portion deemed to be invalid will be deemed omitted, and the remainder of the Agreement shall remain enforceable.

(e) NOTICE. All notices shall be in writing and shall be deemed to be delivered when received by certified mail, postage prepaid, return receipt requested. All notices shall be directed to the parties at the respective addresses set forth below or to such other address as either party may, from time to time, designate by written notice to the other party.

(f) AMENDMENT. No amendment, change, waiver, or discharge hereof shall be valid unless in writing and signed by both parties.

(g) GOVERNING LAW. This Agreement is made in and shall be governed in all respects by the laws of the State of California without regard to its conflict of laws provisions.

(h) ENTIRE AGREEMENT. This Agreement and its Exhibits, which are incorporated herein by this reference, constitute the complete and exclusive statement of all mutual understandings between the parties with respect to the subject matter hereof, superseding all prior or contemporaneous proposals, communications, and understandings, oral or written.

IN WITNESS WHEREOF, the undersigned have duly executed this Agreement, or have caused this Agreement to be duly executed on their behalf, as of _ _[*effective date*]_ _**.**

Date: _ _ _ _ _ _

_ _[*NAME OF CUSTOMER*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _
_ _[*Customer's address*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

Date: _ _ _ _ _ _

_ _[*NAME OF HOST*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _
_ _[*Host's address*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

EXHIBIT A

[*Reproduction of Banner Ad*]

[*Description of Monthly Reports*]

[*Timing and Frequency of Display*]

[*Fees and Payment Terms*]

EXHIBIT B

[*Description of Company's Technical Standards*]

© The Regents of the University of California

§17.33 D. Internet Service Directories or Referral Sites

As the Internet has expanded, the quantity of information accessible over the Internet has grown exponentially and the Internet has become increasingly difficult to navigate. To help users find their way around, so-called referral sites or Internet directories have proliferated. These sites aggregate information about sellers of goods and services, sometimes permitting prospective buyers to comparison shop. The sample agreement in §17.34 is intended for use by a vendor to contract with such a referral site.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/17 Advertising on the Internet/§17.34 E. Form: Internet Advertising Agreement

§17.34 E. Form: Internet Advertising Agreement

To download **Word** version, right click and choose *Save Target As*

To download **WordPerfect** version, right click and choose *Save Target As*

INTERNET ADVERTISING AGREEMENT

This INTERNET ADVERTISING AGREEMENT ("Agreement") is entered into as of _ _[*effective date*]_ _, between_ _[*referral service provider*]_ _ ("Provider"), with offices at _ _[*address*]_ _, and _ _[*customer*]_ _, a _ _[*state of incorporation*]_ _ corporation ("Customer"), with offices at_ _[*address*]_ _.

WHEREAS, Provider operates a website on the Internet located at _ _[*website address*]_ _ (the "Website"), through which Provider desires to provide to Customer the service of advertising Customer's goods and/or services; and

WHEREAS, Customer desires to obtain from Provider the service of advertising Customer's goods and/or services on and through the Website;

NOW THEREFORE, in consideration of the mutual promises contained herein, the parties, intending to be legally bound, agree as follows:

1. SERVICES. Subject to the terms and conditions of this Agreement, Provider agrees to provide to Customer the advertising services ("Services") set forth in Exhibit A. In return, Customer agrees to promptly pay the fees for the provision of the Services, as more fully detailed in Exhibit B. Subject to the terms and conditions of this Agreement, Provider shall use commercially reasonable efforts to provide the Services 24 hours a day, 7 days a week, throughout the term of this Agreement. Customer agrees that from time to time the Services may be inaccessible or inoperable for any reason, including, without limitation: (a) equipment malfunctions; (b) periodic maintenance procedures or repairs that Provider may undertake from time to time; or (c) causes beyond the control of Provider and that are not reasonably foreseeable by Provider, including, without limitation, interruption or failure of telecommunication or digital transmission links, terrorism, hostile network attacks, network congestion, or other failures.

Comment: Often, Internet advertising services are provided in a menu format with pricing variable according to the level or type of service required. For example, premium pricing could be imposed for a more prominent listing or for including links to the customer's site or to additional sources of information. The parties should consider including a provision in the agreement to enable the customer to add or modify services during the contract term without having to execute a new contract.

2. DELIVERY AND PERFORMANCE. Within 30 days of the Effective Date, Customer shall deliver the text, images, logos, and graphics it desires to be published on the Website (the "Data") to Provider in such file formats and on such media as specified by Provider in writing. Within 15 days of Customer's delivery of the Data in specified formats/media, Provider shall commence performance of the Services. Customer acknowledges that Provider shall not be responsible for any delays in Provider's performance of the Services in the event Customer fails to deliver the Data in substantial conformance with Provider's requirements.

3. LICENSE. Solely in connection with Provider's performance of this Agreement, Customer grants to Provider a limited, nontransferable, nonexclusive, worldwide license, for the term of this Agreement to: (a) copy, use, store, publicly display, publicly perform, and transmit the Data on the Website; (b) incorporate the hypertext reference links in the Data on the Website; and (c) display Customer's trade names, trademarks, or service marks on the Website in connection with the Data. The license granted herein permits Provider to make backup copies of the Data and make copies of the Data in connection with mirroring the Site.

4. PROPRIETARY RIGHTS

4.1. CUSTOMER OWNERSHIP. Customer shall retain all right, title, and interest in the Data and all intellectual property rights therein, Customer's trade names, trademarks, logos and service marks, derivative works, modifications, and enhancements thereto, whether or not developed by Customer or any contractor, subcontractor, or agent for Customer.

4.2. PROVIDER OWNERSHIP. Except as provided in the preceding section, Customer acknowledges that the Website, including, without limitation, all trade names, trademarks, service marks, content, text, images, software, media, and other materials contained therein, is a work or collective work, proprietary to or licensed by Provider, protected under copyright, trademark, and other intellectual property laws.

5. CONTENT RESTRICTIONS. Provider reserves the right, at any time in Provider's sole discretion, to refuse to perform the Services with respect to the Data or any portion thereof that: (a) fails to conform to the format and technical specifications set forth by Provider from time to time; (b) is determined by Provider to be likely to constitute any Lanham Act violation, false designation or origin, false advertising, or unfair competition under the law of any jurisdiction; (c) contains or is alleged to contain any content, work, name, mark, designation, materials, or link that actually or potentially violates any applicable law or regulation or infringes any proprietary, intellectual property, contract, or tort right of any person; (d) contains any content, work, name, mark, designation, materials, or link that, to a reasonable person, may be abusive, obscene, pornographic, defamatory, harassing, grossly offensive, vulgar, threatening, or malicious; or (e) contains any

software viruses or any other computer code, files, or programs designed to interrupt, destroy, or limit the functionality of any computer software or hardware or telecommunications equipment.

6. WARRANTIES

6.1. CUSTOMER'S WARRANTIES. Customer represents and warrants to Provider that: (a) Customer has the right and authority to enter into and perform its obligations under this Agreement; (b) the Data will comply with applicable laws; (c) the Data does not contain any content, work, name, logo, or mark that infringes any intellectual property right of any person; (d) the Data does not and shall not contain any software viruses or any other computer code, files, or programs designed to interrupt, destroy, or limit the functionality of any computer software or hardware or telecommunications equipment; and (e) Customer owns the Data and all intellectual property rights therein, or has the right to grant the license to Provider herein and authorize the worldwide copying, display, and transmission of the Data via the Website.

6.2. PROVIDER'S WARRANTIES. Provider represents and warrants to Customer that (a) Provider has the power and authority to enter into and perform its obligations under this Agreement; and (b) Provider shall perform its obligations under this Agreement in a commercially reasonable manner.

7. DISCLAIMER. OTHER THAN AS SPECIFICALLY PROVIDED HEREIN, THE SERVICES AND WEBSITE ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. PROVISION AND/OR USE OF THE SERVICES OR WEBSITE ARE AT CUSTOMER'S SOLE RISK. PROVIDER DOES NOT WARRANT THAT THE SERVICES OR WEBSITE WILL BE UNINTERRUPTED OR ERROR FREE, NOR DOES PROVIDER MAKE ANY WARRANTY AS TO THE PERFORMANCE OR ANY RESULTS THAT MAY BE OBTAINED BY USE OF THE SERVICES OR WEBSITE.

8. LIMITATION OF LIABILITY. EXCLUSIVE OF LIABILITY UNDER SECTION 11 (INDEMNIFICATION), IN NO EVENT SHALL PROVIDER BE LIABLE TO CUSTOMER OR ANY OTHER PERSON FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, INCLUDING LOSS OF PROFIT OR GOODWILL, FOR ANY MATTER ARISING OUT OF OR RELATING TO THIS AGREEMENT AND ITS SUBJECT MATTER, WHETHER SUCH LIABILITY IS ASSERTED ON THE BASIS OF CONTRACT, TORT, OR OTHERWISE, EVEN IF PROVIDER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL PROVIDER'S TOTAL LIABILITY FOR DIRECT DAMAGES EXCEED THE TOTAL FEES PAID BY CUSTOMER TO PROVIDER HEREUNDER.

9. INDEMNIFICATION

9.1. BY CUSTOMER. Customer agrees to indemnify, hold harmless, and defend Provider and its directors, officers, employees, and agents from and against any action, claim, demand, dispute, or liability, including reasonable attorney fees, arising from or relating to (a) any allegation that Customer has engaged in conduct, which if true would breach its warranties or obligations under this Agreement; and (b) any third party claims relating to Customer's products or services.

9.2. BY PROVIDER. Provider agrees to indemnify, hold harmless, and defend Customer and its directors, officers, employees, and agents from and against any action, claim, demand, dispute, or liability, including reasonable attorney fees, arising from or relating to any allegation that Provider has engaged in conduct, which if true would breach its warranties or obligations under this Agreement.

10. TERM AND TERMINATION

10.1. TERM. The term of this Agreement shall commence on _ _[*effective date*]_ _and shall continue for 1 year, unless sooner terminated as set forth herein. The term of this Agreement shall automatically renew thereafter for successive and consecutive 1-year terms unless either party provides written notice of its desire not to renew to the other party at least 60 days prior to the expiration of the then current term.

10.2. TERMINATION. This Agreement may be terminated: (a) by either party on 60 days' written notice to the other party; (b) by Provider, immediately on notice to Customer, on Provider's reasonable belief that Customer has engaged in conduct that if true would breach Customer's warranties under Section 6.1 above.

Comment: The 60-day termination clause effectively assures the customer that pricing will not change for 60 days. Depending on the customer's leverage in the transaction, it may be possible to negotiate a longer price guarantee. From the provider's standpoint, this clause constitutes its only guarantee that the customer will remain on the site for a period of time, in this case 60 days. This may not facilitate the provider's business model for revenue generation. In general, flexibility is advantageous on the Internet, but the length of the term of these agreements can be a factor that does not support a party's business plan. Termination issues should be carefully reviewed.

10.3. PAYMENT ON TERMINATION. In the event this Agreement is terminated, Customer shall pay Provider for all Services undertaken in performance of its obligations hereunder up to the date of termination. Such payment is due and payable within 30 days following such termination.

11. TAXES. Customer shall be solely responsible for and shall pay all sales, use, service, or other taxes, duties, or levies of any governmental entity (exclusive of taxes on Provider's net income), including interest and penalties thereon, if any, relating to the Services, whether or not stated in any invoice to Customer.

12. GENERAL

12.1. INDEPENDENT CONTRACTORS. The parties to this Agreement and their respective personnel are and

shall be independent contractors, and neither party by virtue of this Agreement shall have any right, power, or authority to act or create any obligation, express or implied, on behalf of the other party.

12.2. ASSIGNMENT. Neither party may assign its rights, duties, or obligations under this Agreement to any person or entity, in whole or in part without the prior written consent of the other party; such consent shall not be unreasonably withheld.

12.3. WAIVER. No waiver of any provision hereof or of any right or remedy hereunder shall be effective unless in writing and signed by the party against whom such waiver is sought to be enforced. No delay in exercising, no course of dealing with respect to, or no partial exercise of any right or remedy hereunder shall constitute a waiver of any other right or remedy, or future exercise thereof.

12.4. SEVERABILITY. If any provision of this Agreement is determined to be invalid under any applicable statute or rule of law, it is to that extent to be deemed omitted, and the balance of the Agreement shall remain enforceable.

12.5. AMENDMENT. No amendment, change, waiver, or discharge hereof shall be valid unless in writing and signed by both parties.

12.6. NOTICES. All notices shall be in writing and shall be deemed to be delivered when received by certified mail, postage prepaid, return receipt requested. All notices shall be directed to the parties at the respective addresses set forth below or to such other address as either party may, from time to time, designate by written notice to the other party.

12.7. GOVERNING LAW. This Agreement has been executed in the State of California, and shall be governed in all respects by the laws of the State of California, without regard to its conflict-of-laws rules.

12.8. ENTIRE AGREEMENT. This Agreement, together with its Exhibits, which are incorporated by reference, constitutes the complete and exclusive statement of all mutual understandings between the parties with respect to the subject matter hereof, superseding all prior or contemporaneous proposals, communications, and understandings, oral or written.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed in duplicate as of the date first above written.

Date: _ _ _ _ _ _

_ _[*NAME OF PURCHASER*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _
_ _[*Purchaser's address*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

Date: _ _ _ _ _ _

_ _[*NAME OF SERVICE PROVIDER*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _
_ _[*Service Provider's address*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

EXHIBIT A

SERVICES

The following Services shall be furnished by Provider:

1. BASIC LISTING

Customer's name, address, phone number, and contact information, in addition to e-mail and website links, will be posted on the Website. Customer has the opportunity to be listed in multiple categories of Customer's choice through online account management features; a password will be provided to Customer on execution of this Agreement. New categories may be created only at the discretion of the Provider. All changes to Customer's listing are subject to approval by Provider.

2. PROFILE LISTING

The Profile Listing provides Customer the opportunity to post a _ _[*number*]_ _-character mission statement or company history as well as a corporate logo web link for increased visibility.

3. PRODUCT LISTING

The Product Listing permits Customer to describe up to _ _[*number*]_ _ individual products or services using up to _ _[*number*]_ _ characters for each product or service and to post a full-color photo (a thumbnail size and regular size image (JPEG or GIF format) not wider than _ _[*number*]_ _ pixels) for each product or service.

EXHIBIT B

© The Regents of the University of California

§17.35 F. Portal Agreements

Another method of advertising on the Internet is to arrange with a portal for advertisements that are more fully integrated into the portal's content, such as articles, frames, pop-up ads, and sometimes even e-mail blasts. This arrangement may be tied to a specific event or product launch or may continue for a period of time. Given the closer relationship between the parties, portal agreements (sometimes called marketing agreements) tend to be more complex than other Internet advertising agreements. Marketing agreements may extend to outsourcing of different lines of business or content distribution. For example, a portal may contract with another website to be the exclusive content source for movie reviews and ticket purchasing and enter into cross-promotional relationships that support this arrangement.

The agreement in §17.36 lays out the basic framework for a portal relationship by which the contracting party's products and services are promoted on the portal site with users "pushed through" to the contracting party's site for actual purchase of goods and services.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/17 Advertising on the Internet/§17.36 G. Form: Interactive Marketing Agreement

§17.36 G. Form: Interactive Marketing Agreement

To download **Word** version, right click and choose *Save Target As*

To download **WordPerfect** version, right click and choose *Save Target As*

INTERACTIVE MARKETING AGREEMENT

THIS INTERACTIVE MARKETING AGREEMENT (the "Agreement"), dated _ _[*effective date*]_ _, is between _ _[*company*]_ _ ("Company"), a corporation, with offices at_ _[*company address*]_ _, and _ _[*partner company*]_ _ ("Marketing Partner" or "Advertising Partner"), a _ _[*state of incorporation*]_ _ corporation, with offices at_ _[*partner company address*]_ _. Company and Advertising Partner may be referred to individually as a "Party" and collectively as the "Parties."

NOW THEREFORE, in consideration of the mutual promises contained herein, the parties, intending to be legally bound, agree as follows:

1. PROMOTION, DISTRIBUTION AND MARKETING

1.1. COMPANY PROMOTION OF ADVERTISING PARTNER SITE. Company will provide Advertising Partner with promotional activity for the Advertising Partner Site described on Exhibit A attached hereto (the "Promotions") on Company's portal site located at _ _[*company website address*]_ _ (the "Company Network"). Notwithstanding the terms of Exhibit A, Company does not guarantee any placement in a specific area of the Company Site and, subject to Advertising Partner's reasonable approval, Company will have the right to fulfill its promotional commitments by providing Advertising Partner with comparable promotional placements in appropriate alternative areas of the Company Network. If Company is unable to deliver any particular Promotion, Company will work with Advertising Partner to provide Advertising Partner, as its sole remedy, a comparable promotional placement. Company reserves the right to redesign or modify the organization, structure, "look and feel," navigation, and other elements of the Company Network at any time. In the event such modifications materially and adversely affect any specific Promotion, Company will work with Advertising Partner to provide Advertising Partner, as its sole remedy, a comparable promotional placement.

1.2. CONTENT OF PROMOTIONS. The Promotions will link only to the Advertising Partner Site and will promote only the Advertising Partner Products described in Exhibit A. The specific Advertising Partner Content to be contained within the Promotions described in Exhibit A (the "Promo Content") will be determined by Advertising Partner, subject to Company's technical limitations, the terms of this Agreement, and Company's then-applicable policies relating to advertising and promotions. Advertising Partner will submit in advance to Company for its review a quarterly online marketing plan with respect to the Advertising Partner Site. The Parties will meet in person or by telephone at least monthly to review operations and performance hereunder. Advertising Partner will update the Promo Content no less than every _ _[*number*]_ _ days. Except to the extent expressly described herein, the specific form, placement, duration, and nature of the Promotions will be as determined by Company in its reasonable editorial discretion.

2. ADVERTISING PARTNER SITE

2.1. CONTENT. Advertising Partner will make available through the Advertising Partner Site the Products and related Content described on Exhibit A. Except as mutually agreed in writing by the Parties, the Advertising Partner Site will contain only Content that is directly related to the Advertising Partner Products listed on Exhibit A and will not contain any third party products, services, programming, or other Content. All sales of Products through the Advertising Partner Site will be conducted through a direct sales format; Advertising Partner will not promote, sell, offer, or otherwise distribute any products through any format other than a direct sales format (*e.g.,* through auctions or clubs) without the prior written consent of Company. Advertising Partner will ensure that the Advertising Partner Site does not in any respect promote, advertise, market, or distribute the products, services, or content of any other Interactive Service, or any entity reasonably construed to be in competition with any third party with which Company has an exclusive relationship.

2.2. TECHNOLOGY. Advertising Partner will take all reasonable steps necessary to conform its promotion and sale of Products through the Advertising Partner Site to the then-existing technologies identified by Company which are optimized for the Company Service including, without limitation, any "quick checkout" tool that Company may implement to facilitate purchase of products by Company Users through the Advertising Partner Site. Company will be entitled to require reasonable changes to the Content within any linked pages of the Advertising Partner Site to the extent such Content will, in Company's good faith judgment, adversely affect any operational aspect of the Company Network. Company reserves the right to review and test the Advertising Partner Site from time to time to determine whether the site is compatible with Company's then-available client and host software and the Company Network.

2.3. PRICING AND TERMS. Advertising Partner will ensure that: (a) the prices for Products in the Advertising Partner Site do not exceed the prices for the Products or substantially similar Products offered by or on behalf of Advertising Partner through any other channel of distribution; (b) the terms and conditions related to Products in the Advertising Partner Site are no less favorable in any respect to the terms and conditions for the Products or substantially similar Products offered by or on behalf of Advertising Partner through any Additional Advertising Partner Channel; and (c) both the prices and the terms and conditions related to Products in the Advertising Partner Site are reasonably competitive in all material respects with the prices and terms and conditions for the Products or substantially similar Products offered by any Advertising Partner

competitor through any other interactive site.

Comment: This sort of competitive pricing guarantee may be difficult to adhere to and may result in a company breaching this agreement without knowing it or being able to control the situation. One solution is to require the portal, prior to claiming breach, to provide the company with notice and details of any lower-priced item and an opportunity to cure.

2.4. EXCLUSIVE OFFERS/MEMBER BENEFITS. Advertising Partner shall promote through the Advertising Partner Site on a regular and consistent basis special offers exclusively available to Company Users, such as a meaningful price discount, product enhancement, unique service benefit, or other special feature (the "Company Exclusive Offers"). Advertising Partner shall, at all times, feature at least one Company Exclusive Offer for Company Users per _ _[*number*]_ _-month period.

2.5. OPERATING STANDARDS. Advertising Partner will ensure that the Advertising Partner Site complies at all times with the standards set forth in Exhibit B. To the extent site standards are not established in Exhibit B with respect to any aspect or portion of the Advertising Partner Site (or the Products or other Content contained therein), Advertising Partner will provide such aspect or portion at a level of accuracy, quality, completeness, and timeliness that meets or exceeds prevailing standards in the industry.

2.6. ADVERTISING SALES. As soon as reasonably practical following the Effective Date, the parties will mutually agree on a written advertising program (the "Ad Program") whereby both Company and Advertising Partner will, in coordination with each other, establish advertising inventory space within and sell promotions, advertisements, links, pointers, or similar services or rights through the Advertising Partner Site ("Advertisements"), subject to Company's then-applicable advertising policies and Company's prior approval.

2.7. TRAFFIC FLOW. Advertising Partner will take reasonable efforts to ensure that Company traffic is either kept within the Advertising Partner Site or channeled back into the Company Network (with the exception of advertising links sold and implemented under the Agreement). The Parties will work together on implementing mutually acceptable links from the Advertising Partner Site back to the Company Service. In the event that Company points to the Advertising Partner Site or any other Advertising Partner Interactive Site or otherwise delivers traffic to such site hereunder, Advertising Partner will ensure that navigation back to the Company Network from such site, whether through a particular pointer or link, the "back" button on an Internet browser, the closing of an active window, or any other return mechanism, shall not be interrupted by Advertising Partner through the use of any intermediate screen or other device not specifically requested by the user.

Comment: Consider the extent to which this arrangement is intended to be exclusive between the parties with respect to market segment or to particular types of products. An exclusive relationship should be tied to the achievement of tangible milestones or results; the risk of tying up valuable assets or space on the portal site for a nonperforming relationship could be costly.

3. PAYMENTS

3.1. PAYMENTS. Advertising Partner will pay Company a nonrefundable guaranteed payment of _ _[*dollar amount*]_ _ as follows: _ _[*dollar amount*]_ _ on execution of this Agreement and a payment of _ _[*dollar amount*]_ _ per quarter thereafter during the term hereof. In addition, transaction revenues and advertising revenues will be shared subject to the arrangement set forth on Exhibit C.

3.2. LATE PAYMENTS. All amounts owed hereunder not paid when due and payable will bear interest from the date such amounts are due and payable at the prime rate in effect at such time.

3.3. AUDITING RIGHTS. Advertising Partner will maintain complete, clear, and accurate records of all expenses, revenues, and fees in connection with the performance of this Agreement. For the sole purpose of ensuring compliance with this Agreement, Company (or its representative) will have the right to conduct a reasonable and necessary inspection of portions of the books and records of Advertising Partner that are relevant to Advertising Partner's performance under this Agreement. Any such audit may be conducted after 20 business days' prior written notice to Advertising Partner. Company shall bear the expense of any audit conducted under this Section 4.5 unless such audit shows an error in Company's favor amounting to a deficiency to Company in excess of 5% of the actual amounts paid and/or payable to Company hereunder, in which event Advertising Partner shall bear the reasonable expenses of the audit. Advertising Partner shall pay Company the amount of any deficiency discovered by Company within 30 days after receipt of notice thereof from Company.

Comment: The audit rights in this subsection allow only the portal to audit its contracting partner. Consider whether mutual audit rights are more appropriate for pricing as well as operational performance of the agreement.

3.4. TAXES. Advertising Partner will collect and pay, and indemnify and hold Company harmless from, any sales, use, excise, import or export value-added, or similar tax or duty not based on Company's net income, including any penalties and interest, as well as any costs associated with the collection or withholding thereof, including attorney fees.

3.5. REPORTS. Each payment to be made by Advertising Partner will be accompanied by a report containing information that supports the payment, including information identifying (a) gross Transaction Revenues and all items deducted or excluded from gross Transaction Revenues to produce Transaction Revenues, including, without limitation, chargebacks and credits for returned or canceled goods or services (and, when possible, an explanation of the type of reason therefor, *e.g.,* bad credit card information, poor customer service), and (b) any applicable Advertising Revenues. Company acknowledges that such reports may contain Confidential Information as defined herein.

4. TERM, RENEWAL AND TERMINATION

4.1. TERM. Unless earlier terminated as set forth herein, the initial term of this Agreement will be _ _[*number*]_ _ years from the Effective Date (the Initial Term). On conclusion of the Initial Term, Company will have the right to renew the Agreement for successive 1-year renewal terms (each a Renewal Term and together with the Initial Term, the Term) unless either party provides notice of its intent not to renew within _ _[*number*]_ _ days prior to the expiration of the then current Term.

Comment: Consider how pricing or performance thresholds may need to be adjusted for renewal terms. Further consider whether exclusivity or other special rights or obligations should apply in any renewal term.

4.2. TERMINATION FOR BREACH. Except as expressly provided elsewhere in this Agreement, either Party may terminate this Agreement at any time in the event of a material breach of the Agreement by the other Party that remains uncured after 30 days' written notice thereof to the other Party (or such shorter period as may be specified elsewhere in this Agreement); provided that Company will not be required to provide notice to Advertising Partner in connection with Advertising Partner's failure to make any payment to Company required hereunder, and the cure period with respect to any scheduled payment will be 15 days from the date for such payment provided for herein. Notwithstanding the foregoing, in the event of a material breach of a provision that expressly requires action to be completed within an express period shorter than 30 days, either Party may terminate this Agreement if the breach remains uncured after written notice thereof to the other Party.

4.3. TERMINATION FOR BANKRUPTCY/INSOLVENCY. Either Party may terminate this Agreement immediately following written notice to the other Party if the other Party (a) ceases to do business in the normal course; (b) becomes or is declared insolvent or bankrupt; (c) is the subject of any proceeding related to its liquidation or insolvency (whether voluntary or involuntary) that is not dismissed within 90 calendar days; or (d) makes an assignment for the benefit of creditors.

Comment: Consider whether it is appropriate to include termination for change of control of either party. Additional termination rights could be tied to the failure of the program to meet specified milestones such as dollar values or number of impressions generated.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed in duplicate as of the date first above written.

Date: _ _ _ _ _ _

_ _[*NAME OF COMPANY*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

Date: _ _ _ _ _ _

_ _[*NAME OF PARTNER COMPANY*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

EXHIBIT A

[*Description of Promotions, Products, and Content*]

EXHIBIT B

[*Advertising Partner Website Standards*]

EXHIBIT C

[*Allocation of Transaction Revenues*]

© The Regents of the University of California

18

Viruses and Other Network Disruptions

I. TYPES OF CYBERATTACKS §18.1

II. LEGAL LANDSCAPE §18.2
- A. Federal Legislation
  - 1. Computer Fraud and Abuse Act
    - a. Overview §18.3
    - b. As Applied to Spam §18.4
    - c. As Applied to Conduct Exceeding Terms of Use §18.5
    - d. As Applied to Tracking Software §18.6
    - e. As Applied to Improper Use of E-mail §18.7
    - f. As Applied to Wireless Networks §18.7A
  - 2. Electronic Communications Privacy Act
    - a. Overview §18.8
    - b. As Applied to Cookies §18.9
    - c. As Applied to Tracking Software §18.10
  - 3. Stored Communications Act §18.11
  - 4. As Applied to Unauthorized Wireless Access §18.11A
  - 5. USA Patriot Act §18.12
  - 6. Digital Millennium Copyright Act §18.13
  - 7. Other Federal Statutes §18.14
- B. State Legislation
  - 1. Civil Code §1798.82; Notice of Security Breach; Civil Code §1798.81.5 §18.15
  - 2. Penal Code §502: Computer Crimes §18.16
  - 3. Wireless Devices §18.16A
- C. Trespass to Chattels §18.17
  - 1. *eBay Inc. v Bidder's Edge, Inc.* §18.18
  - 2. *Register.com, Inc. v Verio* §18.19
  - 3. *Intel Corp. v Hamidi* §18.20
  - 4. *Sotelo v DirectRevenue, LLC* §18.20A
  - 5. *Ticketmaster Corp. v Tickets.com, Inc.* §18.21
  - 6. *Thrifty-Tel, Inc. v Bezenek* §18.21A

III. HOW TO RESPOND TO AN ATTACK
- A. General Considerations §18.22
- B. Checklist: Responding to a Cyberattack §18.23

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/18 Viruses and Other Network Disruptions/§18.1 I. TYPES OF CYBERATTACKS

§18.1 I. TYPES OF CYBERATTACKS

As computer systems become more complex, more widely dispersed, and more networked, they are increasingly vulnerable to attack. Intricate layers of hardware and software mean new avenues of potential exploitation for those intent on causing network and system disruptions. "Always on" DSL and other high-speed Internet connections have resulted in increased connectivity, providing more opportunities for hackers and making defensive technologies more difficult to implement. Hacking techniques can be complex, requiring an understanding of computer programming that the average user often does not have. Major threats to computer systems and networks include the following:

- **Computer virus:** A virus is a program or piece of code that is loaded onto a computer or server and runs without the owner's knowledge or consent. A virus cannot enter a computer on its own. It is carried through a host program downloaded from the Internet or copied from another computer, diskette, or other storage medium. A worm is a type of virus that spreads on its own without human assistance. It resides in a computer's memory and uses that memory to replicate itself and travel to other computer hosts. Worms can be contained in very small files; for example, the widely destructive Sapphire worm consisted of only 376 bytes of code.
- **Trojan horse:** A Trojan horse is a malevolent program masked within another program that appears benign. A computer or network accepts a Trojan horse because the program is read and recognized as beneficial to the system. Once accepted, however, the hidden program runs and can cause damage or allow a third party to take over the computer or system remotely. The term "Trojan horse" does not normally refer to programs like viruses or worms that replicate and spread themselves using the host computer as a base.
- **Bomb:** A bomb will lie dormant and then "detonate" on a specific predetermined event. A logic bomb can be triggered by a date, the number of times a program is executed, a random number, or a specific event such as accessing an employee's payroll record. Bombs have been programmed to change random bytes of data on a disk or to wipe out an entire hard drive.
- **Denial of Service attacks ("DoS" attacks):** DoS attacks do not actually yield any information or provide access to a company's systems; instead, they are intended to put the targeted Internet service offline and disrupt its operations. There are various types of DoS attacks, but they generally fall into three categories:
- **Operating system attacks:** Attacks against a certain known fault or weakness of the target computer's operating system. The objective of these attacks is to cause the system to freeze or completely restart. Installing software updates or patches that are released by software manufacturers or independent developers can help prevent against operating system attacks.
- **Networking attacks:** Attacks that attempt to take advantage of built-in aspects of the networking functions of a system, causing it to shut down. The most common type of networking attack directs such a large quantity of data at the network interfaces of the targeted system that it closes down completely or resets the network interface. One version of this tactic is to send incomplete or malicious data packets to computers on a network. Consuming valuable network resources, connected computers become unusable as they attempt to process the corrupted information sent to them.
- **Distributed Denial of Service Attacks (DDoS):** Hackers employ this method by gaining unauthorized access to other computers through various weaknesses and vulnerabilities. Once the machines are accessed, the hacker is able to seize control of them to mount a coordinated denial of service attack on an increased scale because of the use of multiple computers.

Examples of large-scale cyberattacks occurred twice in 2001. The "Code Red" worm, targeting the White House website, impacted more than 250,000 computers over a 2-week period. The "Code Red" worm did not harm individual computers by wiping out files; instead, it took control of computers and used them to generate massive Internet traffic. The second incident, the "Nimda" worm, hit days after the September 11 terrorist attacks in New York, Washington, D.C., and Pennsylvania.

Another large attack occurred in 2003 when the "Sapphire" worm (also known as "Slammer" and "SQLExp") hit over

120,000 computers and negatively affected many corporate networks and Internet service providers. Although the virus did not infect as many systems as Code Red or Nimda, it spread across the Internet so quickly that network administrators could not respond fast enough and some companies lost their Internet connections entirely.

In 2008, a fake media file containing a Trojan horse was detected on more than 500,000 computers. See http://news.bbc.co.uk/2/hi/technology/7389529.stm. The file was disguised as part of media files, including music and video files. Users who tried to play the media files were prompted to install software in order to play the file. However, instead of playing the media, the code generated a barrage of popup advertisements on the user's computer.

In 2009, a computer hacker, Albert Gonzales, pleaded guilty to the theft of "tens of millions of" credit and debit card numbers and related data from major U.S. retailers such as TJX, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, 7-Eleven, and Hannaford Brothers. Gonzales was indicted in separate actions in Massachusetts, New York, and New Jersey. http://www.usatoday.com/tech/news/2009-09-11-gonzalez-hacker-guilty_N.htm.

© The Regents of the University of California

§18.2 II. LEGAL LANDSCAPE

Lawmakers have responded vigorously to the proliferation of viruses, malicious code, and hacking activities over the Internet. Sections 18.3-18.21 briefly summarize applicable federal and state legislation and discuss some recent court decisions of interest to private businesses. The Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice maintains a website directed to computer crime, with policy statements, case law, and guidance for prosecutors and investigators. See http://www.cybercrime.gov.

© The Regents of the University of California

A. Federal Legislation

1. Computer Fraud and Abuse Act

§18.3 a. Overview

The Computer Fraud and Abuse Act (CFAA) (18 USC §1030) was enacted in 1984 to address computer crimes and has been amended to keep pace with advances in technology. For a helpful review of the legislative history of the CFAA, see *Shurgard Storage Ctrs., Inc. v Safeguard Self Storage, Inc.* (WD Wa 2000) 119 F Supp 2d 1121.

The CFAA defines a series of computer-related crimes, including intentionally accessing a computer without authorization (or exceeding authorized access) and thereby obtaining confidential information or anything of value, perpetrating a fraud, or causing other damage. See 18 USC §1030(a). Under the CFAA, insiders who are authorized to access a computer face criminal liability only if they intend to cause damage to the computer, not for recklessly or negligently causing damage. In contrast, outside hackers who break into a computer can be punished for any intentional, reckless, or other damage they cause. See *In re AOL, Inc. Version 5.0 Software Litig.* (SD Fla 2001) 168 F Supp 2d 1359, 1370, quoting S Rep No. 104-357 (1996).

In addition to criminal penalties, the statute creates a private right of action for compensatory damages or injunctive relief for any person who suffers damages or loss from a violation of the Act. See 18 USC §1030(g). The statute defines damages as "any impairment to the integrity or availability of data, a program, a system, or information" that causes a loss aggregating up to $5000 within a one-year period to one or more persons, impairment of medical care, physical injury, or that threatens public health or safety. 18 USC §1030(c)(4)(A), (e)(8). A "loss" by a victim may include costs sustained for the discovery of the violator's identity and the specific information that was accessed, if that information was protected. *SuccessFactors, Inc. v Softscape, Inc.* (ND Cal 2008) 544 F Supp 2d 975, 981. The CFAA has been applied to address Internet-related conduct, such as spam (unsolicited commercial e-mail), automated tracking of website usage, and certain uses of e-mail by employees. See §§18.4-18.7.

© The Regents of the University of California

§18.4 b. As Applied to Spam

In addition to the Computer Fraud and Abuse Act (CFAA) (18 USC §1030), senders of unsolicited commercial e-mail (also known as UBE, junk e-mail, or spam) are subject to the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act) (Pub L 108-187, 117 Stat 2699, codified primarily at 15 USC §§7701-7713 and 18 USC §1037), as well as any state laws regulating commercial e-mail that are not preempted by the CAN-SPAM Act. See generally §§17.11-17.29.

In *America Online, Inc. v National Health Care Discount, Inc.* (ND Iowa 2000) 121 F Supp 2d 1255, America Online Inc. (AOL) sought to hold the defendant, National Health Care Discount (NHCD), liable under the CFAA (18 USC §1030) and the common law theory of trespass to chattels (see §§18.17-18.21) for the actions of its sales representatives, who bombarded AOL subscribers with an estimated 300 million unsolicited e-mail advertisements over a two-year period. The court found that the sales representatives' conduct violated 18 USC §1030(a)(2)(C), because they intentionally accessed AOL's computers in violation of AOL's terms of service, which prohibited the harvesting of e-mail addresses, and also found that the sales representatives' conduct constituted a trespass to chattels. The sales representatives were AOL subscribers, however, so there was an issue whether their access was "unauthorized" within 18 USC §1030(a). There were also issues whether NHCD's conduct had caused AOL "damage" within the meaning of the CFAA (18 USC §1030(e)(8)(A)), and whether the offending marketers were NHCD's agents (and thereby subject to NHCD's control) or independent contractors. The court therefore denied AOL's motion for summary judgment. After a trial on the remaining issues, the court found that the evidence established as a matter of law that the e-mail marketers were acting as NHCD's agents, that regardless of authorization they had "exceeded authorized access," and that sufficient "damage" had occurred to make out a claim under the CFAA. *America Online, Inc. v National Health Care Discount, Inc.* (ND Iowa 2001) 174 F Supp 2d 890, 897.

© The Regents of the University of California

§18.5 c. As Applied to Conduct Exceeding Terms of Use

America Online, Inc. v National Health Care Discount, Inc. (ND Iowa 2000) 121 F Supp 2d 1255, 1276 (see §18.4), illustrates that violations of a website's terms of use may constitute "exceed[ing] authorized access" for purposes of a civil claim under the Computer Fraud and Abuse Act (CFAA) (18 USC §1030). The CFAA defines "exceeds authorized access" to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." 18 USC §1030(e)(6). Exceeding authorized access to a computer system in order to commit a fraud or to obtain something of value is generally prohibited by 18 USC §1030(a)(4). In *EF Cultural Travel BV v Zefer Corp.* (1st Cir 2003) 318 F3d 58, the court affirmed the issuance of an injunction to prevent the defendant from using an electronic "scraper" tool to collect tour pricing information for one of plaintiff's competitors from the plaintiff's website in violation of the website's terms of use. See also *Creative Computing v Getloaded.com* (9th Cir 2004) 386 F3d 930, 937 (defendant's egregious conduct, including appropriating plaintiff's source code and trade secrets via hacking, justified "extraordinarily broad" injunction prohibiting defendant from accessing plaintiff's website).

In *Therapeutic Research Faculty v NBTY, Inc.* (ED Cal 2007) 488 F Supp 2d 991, 997, denying the defendants' motion to dismiss, the court found that the plaintiff's allegations that defendants shared a single-user password to gain access to one of plaintiff's publications without authorization stated a claim under the CFAA.

In *U.S. v Drew* (CD Cal, May 15, 2008, No. CR-08-0582-GW) (the indictment is available online at http://online.wsj.com/public/resources/documents/Drew.pdf), the defendant, Lori Drew, created a MySpace account under a fake identity, which she used to develop an online relationship with a 13-year-old girl through MySpace services. She used her fake identity to communicate hurtful comments to the girl, who subsequently committed suicide. The defendant was criminally charged with four felonies, including charges under 18 USC §§1030(a)(2)(C) and 1030(c)(2)(B)(ii) for unauthorized use of a computer and unauthorized use of a computer to conduct a tortious act—specifically, to inflict emotional distress. The defendant was prosecuted under the theory that MySpace account holders who violate the company's TOS are exceeding authorized access and thereby violating the CFAA. The jury convicted the defendant on three misdemeanor counts of unauthorized access to a computer. See http://www.nytimes.com/2008/11/27/us/27myspace.html. Drew was subsequently acquitted by a federal court in California, which held that the misdemeanor provisions of the CFAA are unconstitutionally vague when the alleged violation is based on the defendant's intentional violation of a website's terms of service. *U.S. v Drew* (CD Cal 2009) 259 FRD 449, 467. The court raised concern that criminalizing mere violations of a site's terms of use would "convert a multitude of otherwise innocent Internet users into misdemeanant criminals." 259 FRD at 466.

© The Regents of the University of California

§18.6 d. As Applied to Tracking Software

Cases under the Computer Fraud and Abuse Act (CFAA) (18 USC §1030) that involve alleged invasions of privacy may also implicate the Electronic Communications Privacy Act (ECPA) (18 USC §§2510-2522 and 2701-2712) (see §§18.8-18.10) and other federal and state privacy laws. For further discussion of privacy law, see chap 9. The plaintiffs in *In re Pharmatrak, Inc. Privacy Litig.* (D Mass 2002) 220 F Supp 2d 4, rev'd on other grounds (1st Cir 2003) 329 F3d 9, were Internet users whose personal information had been collected by a web tracking service (Pharmatrak) from pharmaceutical company websites without the users' knowledge or consent. The plaintiffs sued Pharmatrak and the pharmaceutical companies who had contracted for its services under the ECPA and the CFAA, alleging that Pharmatrak had illegally intercepted and accessed the plaintiffs' private health information and web browsing habits. Although the plaintiffs' ECPA claims were eventually upheld on appeal (see *In re Pharmatrak, Inc. Privacy Litig.* (1st Cir 2003) 329 F3d 9, discussed in §18.10), the federal district court dismissed the plaintiffs' claims under the CFAA because plaintiffs did not establish that they had suffered damage over the statutory threshold of $5000 in 18 USC §1030(e)(8). The court noted that damages under the CFAA could be aggregated, but only if caused by a "single act" of the defendant. The plaintiffs had not shown that they suffered damages in excess of the statutory threshold on account of a single act by the defendants or that the defendants had the requisite mens rea to be held liable under the Act. See also *In re DoubleClick Inc. Privacy Litig.* (SD NY 2001) 154 F Supp 2d 497. However, the court in *In re AOL, Inc. Version 5.0 Software Litig.* (SD Fla 2001) 168 F Supp 2d 1359, 1373, stated that despite the wording of §1030(a)(5), which requires that the damage threshold must be met "to a protected computer," damages arising from a "single act" affecting multiple computers could be aggregated to meet the $5000 threshold even if the amount was not met for any single computer. See also §18.12.

In *Kalow & Springnut, LLP v Commence Corp.* (D NJ, June 23, 2008, No. 07-3442(FLW)) 2008 US Dist Lexis 48036, the court determined that the intentional transmission of software code, including the possibility of a "time bomb" that would cause the software to stop working at a certain point in time, was insufficient to sustain a cause of action under 18 USC §1030(a)(5)(A)(i) without additional proof that the software code was intended to cause harm to the victim's computer. 2008 US Dist Lexis 48036 at *6.

© The Regents of the University of California

§18.7 e. As Applied to Improper Use of E-mail

The plaintiff and defendant in *Shurgard Storage Ctrs., Inc. v Safeguard Self Storage, Inc.* (WD Wa 2000) 119 F Supp 2d 1121 were competitors in the self-storage industry. The plaintiff (Shurgard) claimed that the defendant engaged in a scheme to hire away some of Shurgard's key employees in order to obtain Shurgard's trade secrets and that some of the employees, while still working for Shurgard, used Shurgard's computers to send trade secrets to the defendant by e-mail. In addition to claims for misappropriation of trade secrets, conversion, unfair competition, and tortious interference with a business expectancy, Shurgard alleged violations of the Computer Fraud and Abuse Act (CFAA) (18 USC §1030), seeking damages and injunctive relief.

The federal district court held that Shurgard's employees exceeded their authorization for purposes of the CFAA (18 USC §1030(a)(2)(C)) in their use of Shurgard's computers by sending confidential information to the defendant. Their authority to access Shurgard's computers ended when they became agents for the defendant under principles of agency law. Quoting from S Rep No. 104-357, at 11 (1996), the court also held that Shurgard had sufficiently alleged damages within the CFAA:

> [I]t is not always clear what constitutes "damage." For example, intruders often alter existing log-on programs so that user passwords are copied to a file which the hackers can retrieve later. After retrieving the newly created password file, the intruder restores the altered log-on file to its original condition. Arguably, in such a situation, neither the computer nor its information is damaged. Nonetheless, this conduct allows the intruder to accumulate valid user passwords to the system, requires all system users to change their passwords, and requires the system administrator to devote resources to resecuring the system. Thus, although there is arguably no "damage," the victim does suffer "loss." If the loss to the victim meets the required monetary threshold, the conduct should be criminal, and the victim should be entitled to relief.

"Damage" under 18 USC §1030(e)(8) is defined to include "any impairment to the integrity… of data… or information." The court found that even though none of Shurgard's data was physically changed or erased by the conduct of its former employees, Shurgard had been damaged because an impairment of the integrity of its data had occurred.

The expansive notion of applying agency law principles to the CFAA was rejected in *Shamrock Foods Co. v Gast* (D Ariz 2008) 535 F Supp 2d 962. Plaintiff Shamrock sued a former employee under the CFAA and several state statutes, alleging that the defendant sent numerous e-mails containing Shamrock's confidential information to his personal account before leaving Shamrock for employment at a competitor. Shamrock claimed that the defendant was acting as an agent for his new employer at the time the confidential information was accessed and e-mailed and that he thereby accessed Shamrock's computers without authorization. Rejecting the view taken in *Shurgard*, the court adopted a narrower application of the CFAA, holding that "without authorization" was intended to apply only to conduct by "outsiders" who do not have permission to access the protected computers to begin with. 535 F Supp 2d at 964. The court noted that "the legislative history confirms that the CFAA was intended to prohibit electronic trespassing, not the subsequent use or misuse of information." 535 F Supp 2d at 966.

The Ninth Circuit took a similar approach in *LVRC Holdings LLC v Brekka* (9th Cir 2009) 581 F3d 1127, a case against an employee who e-mailed documents to himself from his company account after receiving notice of termination of his employment. The court noted that the defendant was still employed when he sent the e-mails, and use of the computer system was a required aspect of his job. The court found that the employee's actions were not covered by the CFAA, holding that (581 F3d at 1135):

> a person uses a computer "without authorization"… when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/18 Viruses and Other Network Disruptions/§18.7A f. As Applied to Wireless Networks

§18.7A f. As Applied to Wireless Networks

Wireless networks continue to grow in popularity because they provide a cheap and convenient method to interconnect multiple computers. Wireless fidelity (Wi-Fi), currently the most popular form of wireless networking, is employed for both personal and business use.

The rise in popularity of Wi-Fi has resulted in increasing numbers of unsecured (and hence vulnerable) networks. Exploitation of wireless networks can range from accessing a neighbor's unsecured network to surf the web to more concerted activity such as hacking into a secured network or "wardriving" (the act of searching for unsecured Wi-Fi networks from a moving vehicle using a portable computer). Combining "wardriving" with transmission of unsolicited bulk e-mail is known as "war spamming." See http://www.fbi.gov/page2/nov04/warspammer111004.htm.

Courts have not yet weighed in on whether the CFAA imposes liability for merely accessing and using an unsecured network. Nonetheless, accessing and using another's wireless network without authorization may violate federal criminal statutes under the CFAA, the Electronic Communications Privacy Act of 1986 (18 USC §§2510-2522 and 2701-2712) (see §18.8), and the Wiretap Act (18 USC §§2510-2522) (see §18.8) and may also constitute a trespass to chattels. See §§18.11A, 18.17.

Under the CFAA, accessing the wireless signal of another arguably constitutes intentionally accessing a computer without authorization (or exceeding authorized access) under 18 USC §1030(a). But §1030(a) imposes two additional elements:

- That the person gaining access obtain confidential information or anything of value; and
- That the person is perpetrating a fraud or causing other damage.

Merely accessing another's network provides access to the packets of information that are carried by the network, and it is therefore possible for a court to find that the requirement for obtaining confidential information or information of value has been met. Access may impose a load on the network, slowing it down or interfering with efficient operation, thereby causing harm. Given the ready availability of security features for commercially available wireless network systems, however, failure to implement reasonable safeguards (such as password protection or encryption) may rebut an argument that access is unauthorized and that the CFAA is implicated.

Criminal convictions in this area have generally involved additional criminal activity beyond mere unauthorized access. The first "war spamming" case in the United States was *U.S. v Tombros*, in which defendant Nicholas Tombros was convicted under the CAN-SPAM Act for spamming in 2004. Tombros pled guilty to sending spam e-mail messages that advertised pornographic Internet sites from his laptop while driving through Venice, California. See http://www.fbi.gov/page2/nov04/warspammer111004.htm.

Another case is *U.S. v Salcedo* (4th Cir 2006) 189 Fed Appx 197 (unpublished), in which defendant Brian Salcedo hacked into the computer system of a Lowe's retail store while sitting in a car in the parking lot, and gained access to Lowe's network to steal credit card account numbers. See http://www.usdoj.gov/criminal/cybercrime/salcedoSent.htm. Salcedo pled guilty to conspiracy to commit wire and computer fraud, fraud activity in connection with computers in violation of the CFAA under 18 USC §1030(a)(5), accessing a computer without authorization and obtaining information from a protected computer involving interstate information in violation of the CFAA under 18 USC §1030(a)(2), and accessing a protected computer without authorization and obtaining a thing of value in violation of the CFAA under 18 USC §1030(a)(4). Despite the absence of concrete case law and federal authority dealing with the legal implications of unauthorized wireless surfing over Wi-Fi networks, the FBI has commented on the growing threat of Wi-Fi hacking. The FBI notes loss of subscription revenue, spying on unguarded computer systems, industrial espionage, counterintelligence, and identity theft as among the threats posed by Wi-Fi hacking. See http://www.fbi.gov/publications/realitytech/realitytech.pdf at 53, 54. Although the legality of wardriving remains undetermined, any claim brought by a victim of a Wi-Fi hacker would still have to satisfy the necessary elements for a cause of action under the CFAA. Current legal and technical articles pertaining to wardriving can be found at http://www.wardriving.com.

© The Regents of the University of California

2. Electronic Communications Privacy Act

§18.8 a. Overview

The Electronic Communications Privacy Act of 1986 (ECPA) (Pub L 99-508, 100 Stat 1848), codified at 18 USC §§2510-2522 and 2701-2712, expanded the scope of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (also known as the Wiretap Act) (Pub L 90-351, 82 Stat 211) to prohibit the unauthorized interception, use, and disclosure of electronic, as well as oral and wire, communications. The ECPA thus extended the privacy protections in the Wiretap Act to cover interception of e-mail and other electronic files, as well as conventional wiretapping and eavesdropping.

The ECPA has two parts: Title I, codified at 18 USC §§2510-2522 and which continues to be known as the Wiretap Act, covers interception of oral, wire, and electronic communications. Significantly, Title I of the ECPA does not cover *stored* electronic communications. It only covers electronic communications intercepted in the course of transmission. *Konop v Hawaiian Airlines, Inc.* (9th Cir 2002) 302 F3d 868, cert denied (2003) 537 US 1193. See also *Fraser v Nationwide Mut. Ins. Co*. (3d Cir 2003) 352 F3d 107. Title II of the ECPA, codified at 18 USC §§2701-2712 and also known as the Stored Communications Act, does cover unauthorized access to wire and electronic communications and transaction records held in storage. The Stored Communications Act is discussed in §18.11. The ECPA was deliberately structured to give electronic communications *in storage* lesser protection than other types of communication. *Konop v Hawaiian Airlines, Inc.* (9th Cir 2002) 302 F3d 868, 877, cert denied (2003) 537 US 1193.

In addition to criminal penalties, Title I of the ECPA creates a private right of action against anyone who, without proper authorization, "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 USC §§2511(1)(a), 2520. The term "intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 USC §2510(4). A plaintiff must prove five elements to make out a claim under Title I of the ECPA: "that the defendant (1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication (5) using a device." *In re Pharmatrak, Inc. Privacy Litig.* (1st Cir 2003) 329 F3d 9, 19. There are statutory exceptions, including, of course, properly authorized interceptions by law enforcement, consent, and routine service or quality control checks by communications service providers in the ordinary course of their operations. See 18 USC §2511.

© The Regents of the University of California

§18.9 b. As Applied to Cookies

A cookie is a piece of software code transmitted by a website server to an Internet user's web browser that the browser software saves and returns to the server whenever the user visits the website again. Cookies may or may not expire after a certain time period. "Persistent" cookies remain stored in a user's web browser after the end of an online session. Reputable online businesses widely use cookies for the convenience of their users. Cookies may store user preferences, registration and login information, and customer information related to online purchases. Cookies may also contain unique codes or identifiers that permit an online business to differentiate among website users. See also §9.4.

Use of cookies may implicate both Title I and Title II of the Electronic Communications Privacy Act (ECPA) (18 USC §§2510-2522 and 2701-2712), as well as the Computer Fraud and Abuse Act (CFAA) (18 USC §1030). Internet users who have asserted violations of the ECPA or the CFAA based on the use of cookies have met with little success, however. See generally *In re Toys R Us, Inc. Privacy Litig.* (ND Cal, Oct. 9, 2001) 2001 US Dist Lexis 16947; *In re Intuit Privacy Litig*. (CD Cal 2001) 138 F Supp 2d 1272; *In re DoubleClick Inc. Privacy Litig.* (SD NY 2001) 154 F Supp 2d 497. Notably, in *Chance v. Avenue A, Inc.* (WD Wash 2001) 165 F Supp 2d 1153, the federal district court ruled that consent by only one party to the interception of an electronic communication (*e.g.*, through use of a cookie) will negate liability under the ECPA, as long as the interception does not have a criminal or tortious purpose. See 18 USC §2511(2)(d). The court found the defendant's consent was sufficient and granted summary judgment for the defendant on plaintiff's ECPA claim.

In re DoubleClick Inc. Privacy Litig., supra, is one of the leading cases analyzing the use of cookies in relation to the ECPA and the CFAA. Defendant DoubleClick is a global leader in Internet advertising products and services. It collects, compiles, and analyzes information about Internet users through the use of cookies and other proprietary technology, and delivers targeted advertising for its clients based on the user information collected. In *DoubleClick,* the federal district court dismissed with prejudice a class action suit against DoubleClick alleging that its placement and use of cookies on plaintiffs' computers violated Titles I and II of the ECPA, the CFAA, and various state laws. The court found that DoubleClick's activities were authorized by the plaintiff Internet users for purposes of the ECPA exceptions in 18 USC §§2511(2)(d) and 2701(c)(2). The court noted that DoubleClick did not access end users' hard drives to gather information, but rather only the data files submitted by users themselves to DoubleClick's clients' websites, and that plaintiffs could easily and at no cost prevent DoubleClick from collecting information from them, either by configuring their browsers to block cookies or by visiting Double-Click's own website and requesting an "opt-out" cookie.

© The Regents of the University of California

§18.10 c. As Applied to Tracking Software

A company can obtain valuable strategic information about its customers by tracking its customers' use of the company's website. In some circumstances, however, website usage tracking may constitute an unauthorized interception of electronic communications under Title I of the Electronic Communications Privacy Act of 1986 (ECPA) (Pub L 99-508), codified at 18 USC §§2510-2522. *In re Pharmatrak, Inc. Privacy Litig.* (1st Cir 2003) 329 F3d 9 is a leading case on the scope of privacy protection afforded Internet users under Title I of the ECPA. As noted in §18.6, defendant Pharmatrak was a web tracking service engaged by a number of pharmaceutical companies to collect information on users of the pharmaceutical companies' websites. Pharmatrak and the pharmaceutical companies were sued by website users under the ECPA (and the Computer Fraud and Abuse Act (CFAA) (18 USC §1030); see §18.6), alleging that Pharmatrak had illegally intercepted and accessed the users' private health information and web browsing habits. The First Circuit found that, for purposes of the ECPA, neither the pharmaceutical companies nor website users had given consent to Pharmatrak's collection of personal information. Further, even under a narrow reading of the ECPA's "interception" requirement (see §18.8), Pharmatrak had intercepted the users' information in "real time," contemporaneously with its transmission by the users.

© The Regents of the University of California

§18.11 3. Stored Communications Act

Title II of the Electronic Communications Privacy Act (ECPA) (18 USC §§2701-2712), known as the Stored Communications Act, is intended to prevent hackers from obtaining, modifying, or destroying stored electronic communications. It establishes criminal penalties and a private right of action against any person who "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system … and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage." 18 USC §§2701(a)(1), 2707(a). "Electronic storage" means "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 USC §2510(17). See *Theofel v Farey-Jones* (9th Cir 2003) 341 F3d 978, 982, reprinted as amended (9th Cir 2004) 359 F3d 1066, 1072, cert denied (2004) 166 L Ed 2d 17. The law exempts access that is authorized by the person or entity providing the wire or electronic communications or the user sending or receiving the communication. 18 USC §2701(c).

In *Konop v Hawaiian Airlines, Inc.* (9th Cir 2002) 302 F3d 868, 877, cert denied (2003) 537 US 1193, an airline pilot (Konop) sued his employer, alleging that the airline had gained unauthorized access to the pilot's secure website, on which he had posted messages critical of the airline and its officers. Two other pilots who were authorized users of the website had given their access codes to a senior airline officer without Konop's knowledge. Among other things, Konop claimed that, by viewing his secure website, the airline had violated the Stored Communications Act. The Ninth Circuit reversed the federal district court's grant of summary judgment for the defendant airline on this point, holding that the airline was not an authorized user of the website within 18 USC §2701(c)(2) because only Konop could grant such authorization.

In *Therapeutic Research Faculty v NBTY, Inc.* (ED Cal 2007) 488 F Supp 2d 991, 997, denying the defendants' motion to dismiss, the court found that the plaintiff's allegations that the defendants shared a single-user password to gain access to one of the plaintiff's publications without authorization stated a claim under the ECPA.

In *Pietrylo v Hillstone Restaurant Group* (D NJ, Sept. 25, 2009, No. 06-5754) 2009 US Dist Lexis 88702, a federal jury in New Jersey determined that an ECPA violation occurred when the defendant, through its managers and without authorization, knowingly, intentionally, or purposefully accessed the "Spec-Tator," a group on MySpace.com for past and present employees of Houston's Restaurant, to "vent" about their employer. Managers accessed the site using the username and password of an employee who testified that she gave her password to management because she felt she probably "would have gotten in trouble" if she had not. The court held that the jury could reasonably infer from such testimony that the employee's purported "authorization" was coerced. 2009 US Dist Lexis 88702 at *8.

Courts have addressed whether web-based e-mails held by an Internet service provider are in "electronic storage" within the meaning of the ECPA. In *Theofel v Farey-Jones* (9th Cir 2003) 359 F3d 1066, 1075, the Ninth Circuit held that the ECPA covers stored e-mail messages:

> An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again, if, for example, the message is accidentally erased from the user's own computer. The ISP copy of the message functions as a "backup" for the user. Notably, nothing in the Act requires that the backup protection be for the benefit of the ISP rather than the user. Storage under these circumstances thus literally falls within the statutory definition.

But see *U.S. v Weaver* (CD Ill 2009) 636 F Supp 2d 769 (opened, web-based e-mails held by Internet service provider are not in "electronic storage" within meaning of ECPA).

© The Regents of the University of California

§18.11A 4. As Applied to Unauthorized Wireless Access

The Electronic Communications Privacy Act (ECPA) (18 USC §§2510-2522 and 2701-2712) does not address unauthorized wireless access directly, and no courts have yet weighed in on the subject. However, certain provisions of the ECPA may be applicable to such activity. The Wiretap Act (Title I of ECPA) (18 USC §§2510-2522) provides for fines and imprisonment of up to 5 years for any person who intentionally intercepts an electronic communication. See 18 USC §2511. "Intercept" is defined under ECPA as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 USC §2510(4). Thus, Wi-Fi hackers may be liable for snooping into private networks, regardless of whether any information gathered from the unauthorized access is recorded. See *Watkins v L.M. Berry & Co.* (11th Cir 1983) 704 F2d 577, 584 ("[t]he violation of §2511(1)(b) is the intercepting itself, not the interception of particular material").

The Pen Register Act (18 USC §§3121-3127) may also apply to certain unauthorized wireless intrusions. The Act prohibits any person from using a pen register or a trap and trace device without first obtaining a court order. 18 USC §3121. A pen register is (18 USC §3127(3)):

> a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication.

© The Regents of the University of California

§18.12 5. USA Patriot Act

Section 814 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act) (Pub L 107-56, 115 Stat 272) addressed "deterrence and prevention of cyber-terrorism" by amending the Computer Fraud and Abuse Act (CFAA) (18 USC §1030), to bring cyberattacks within the definition of "terrorism" and to increase criminal penalties for CFAA violations. The CFAA now allows state convictions to be counted as prior offenses (18 USC §1030(e)(10)) and increases prison sentences up to 20 years (18 USC §1030(c)). Computers located outside the U.S. that can affect U.S. interstate and foreign commerce and communications have been added to the definition of "protected computers" covered by the statute. 18 USC §1030(e)(2)(b).

The Patriot Act also amended the CFAA to allow losses to several computers to be aggregated to meet the $5000 jurisdictional threshold for actionable damages. 18 USC §1030(a)(5)(B)(i). Further, it added a definition from *U.S. v Middleton* (9th Cir 2000) 231 F3d 1207, 1210, for the previously undefined term "loss," to include the costs of responding to the offense, assessing damage, and restoring the system, and the revenue lost because of service interruption or by a user of that service with respect to a communication of or intended for that user.

Section 213 of the Patriot Act also provides for a delay of required notices for the execution of a warrant if the immediate notice could result in adverse consequences, such as the destruction of evidence. See 18 USC §3103a(b).

© The Regents of the University of California

§18.13 6. Digital Millennium Copyright Act

The anti-circumvention provisions of the Digital Millennium Copyright Act (Pub L 105-304, 112 Stat 2860), codified in scattered sections of Title 17 of the United States Code, including 17 USC §§512, 1201-1205, 1301-1332, prohibit circumvention (by conduct or technological devices) of legitimate technological measures to control access to, and to prevent unauthorized reproduction of, copyrighted works. For further discussion of the Digital Millennium Copyright Act, see §§1.22-1.41.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/18 Viruses and Other Network Disruptions/§18.14 7. Other Federal Statutes

§18.14 7. Other Federal Statutes

Rights of action under other federal statutes may be available to Internet service providers, businesses, or individuals who become victims of computer crime, depending on the facts and circumstances of the case. The Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice maintains a website at http://www.usdoj.gov/criminal/cybercrime/cclaws.html, which lists a series of provisions in the United States Code relating to various types of computer crime, including:

- Copyright and copyright management (17 USC §§506, 1201-1205; 18 USC §§2318-2319);
- Bootlegging (18 USC §2319A-2319B);
- Trademarks and trade secrets (18 USC §§1831-1839, 2320);
- Integrity of intellectual property systems (17 USC §506; 18 USC §497);
- Misuse of dissemination systems (18 USC §§1341, 1343, 2512; 47 USC §553, 605);
- Searching and seizing computers (18 USC §§2510, 2701, 3121; 42 USC §2000aa);
- Cyberstalking (18 USC §§875, 2261A; 47 USC §223);
- Fraud in connection with access devices (18 USC §1029);
- Communication lines, stations, or systems (18 USC §1362); and
- Recording of dialing, routing, addressing, and signaling information (18 USC §3121).

© The Regents of the University of California

B. State Legislation

§18.15 1. Civil Code §1798.82; Notice of Security Breach; Civil Code §1798.81.5

Civil Code §1798.82 requires any person doing business in California that maintains computerized personal information on California residents to notify them if their personal data may have been acquired by an unauthorized individual as a result of a security breach. The law is intended to help individuals protect themselves against identity theft. Any person injured by a violation of CC §1798.82 may bring a civil action for damages and injunctive relief. CC §1798.84(b), (e). "Personal information" is defined to include a person's name together with one or more of the following: Social Security number, driver's license or state ID card number, credit card or other financial account numbers, medical information, or health insurance information combined with passwords or access codes, but does not include "publicly available information that is lawfully made available to the general public from federal, state, or local government records." CC §1798.82(e), (f)(1). "Medical information" is defined as any information regarding medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional (CC §1798.82(f)(2)); "health insurance information" pertains to an individual's "health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records" (CC §1798.82(f)(3)). Civil Code §1798.84(a) provides that any attempted waiver of the provisions of CC §1798.82 is against public policy and unenforceable.

NOTE: Civil Code §1798.82(a) applies only to "unencrypted" personal information. In theory, Internet businesses that encrypt all personally identifiable information in their stored records should not be required to give notice in the event of a security breach. See CC §1798.82(a). Civil Code §1798.82(b), however, requires persons or businesses in possession of personal information that they do not own to notify the owner or licensee of the information in the event of a security breach, irrespective of whether the information was encrypted. It is therefore prudent to assume that notice in accordance with statutory procedures is required in case of any security breach, regardless of the status of encryption of the accessed records.

Notice must be given under both CC §§1798.82(a) and 1798.82(b) if personal information was, or is *reasonably believed* to have been, acquired by an unauthorized person. Thus, notice may be required even without concrete evidence that personal information was actually obtained by an unauthorized individual. Notice must be made without unreasonable delay and can be made in writing or electronically. CC §1798.82(g)(1)-(2). The statute provides alternative methods for giving notice if the cost of providing notice would exceed $250,000, the number of persons to be notified exceeds 500,000, or the business does not have sufficient contact information to provide all notices in writing or electronically. CC §1798.82(g)(3).

Personal consumer information received further protection with the enactment of CC §1798.81.5, operative January 1, 2005. Businesses are now expressly required to implement reasonable procedures to maintain the security of personal information that the business stores or discloses to third parties. The statute applies to businesses that own or license personal information about California residents. "Personal information," as defined in the statute, includes an individual's first name or initial and last name in conjunction with the individual's

- Social Security number;
- Driver's license or ID card number;
- Account, credit, or debit card number in combination with the account access code or passwords; or
- Medical information.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/18 Viruses and Other Network Disruptions/§18.16 2. Penal Code §502: Computer Crimes

§18.16 2. Penal Code §502: Computer Crimes

Penal Code §502 is the California statute addressed to computer crimes. It is intended to protect individuals, businesses, and governmental agencies from unauthorized access, tampering, interference, or damage to computer systems and data. Criminal penalties under Pen C §502 include fines of up to $10,000, up to 3 years in jail, or both. Pen C §502(d). In addition to criminal penalties, the statute provides that an owner or lessee of a computer system, network, program, or data who suffers loss or damages from a violation of the statute has the right to bring a civil action against the violator for compensatory damages and injunctive relief. Pen C §502(e)(1). "Compensatory damages" is defined to include "any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access." For purposes of any civil action, a minor's conduct is imputed to the parent or guardian having control or custody of the minor. Pen C §502(e)(1).

The statute lists nine violations, as follows (Pen C §502(c)):

- Knowingly accessing, and without permission altering, damaging, deleting, destroying, or otherwise using, any data, computer, computer system, or computer network, either to devise or execute any scheme or artifice to defraud, deceive, or extort, or to wrongfully control or obtain money, property, or data.
- Knowingly accessing, and without permission taking, copying, or making use of, any data from a computer, computer system, or computer network, or taking or copying any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
- Knowingly and without permission using or causing to be used computer services.
- Knowingly accessing, and without permission adding, altering, damaging, deleting, or destroying, any data, computer software, or computer programs that reside or exist internal or external to a computer, computer system, or computer network.
- Knowingly and without permission disrupting or causing the disruption of computer services, or denying or causing the denial of computer services to an authorized user of a computer, computer system, or computer network.
- Knowingly and without permission providing or assisting in providing a means of accessing a computer, computer system, or computer network in violation of the statute.
- Knowingly and without permission accessing or causing to be accessed any computer, computer system, or computer network.
- Knowingly introducing any computer contaminant into any computer, computer system, or computer network.
- Knowingly and without permission using the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damaging or causing damage to a computer, computer system, or computer network.

A "computer contaminant" is defined as

> any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information [including] but … not limited to, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network. Pen C §502(b)(10).

"Injury" is defined as (Pen C §502(b)(8)).

> any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access, or the denial of access to legitimate users of a computer system, network, or program.

In *Therapeutic Research Faculty v NBTY, Inc.* (ED Cal 2007) 488 F Supp 2d 991, 998, denying the defendants' motion to dismiss, the court found that the plaintiff's allegations that defendants shared a single-user password to gain access to one of plaintiff's publications without authorization stated a claim under Pen C §502.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/18 Viruses and Other Network Disruptions/§18.16A 3. Wireless Devices

§18.16A 3. Wireless Devices

Business and Professions Code §22948.6 requires manufacturers of wireless access points for use in small offices, home offices, and residential settings to advise consumers how to protect their wireless network connection from unauthorized access. The warning must appear in the configuration process of the device or be attached to the device as a temporary sticker that must be removed to allow the device to be used. Bus & P C §22948.6(a)(1)-(2).

© The Regents of the University of California

§18.17 C. Trespass to Chattels

Companies that have had their operations disrupted by viruses, web crawlers, or other forms of malevolent code have used the common law theory of trespass to chattels with limited success to seek redress. As the federal district court in *Ticketmaster Corp. v Tickets.com, Inc*. (CD Cal, Aug. 10, 2000, CV99-7654 HLH) 2000 US Dist Lexis 12987, aff'd without opinion (9th Cir 2001) 248 F3d 1173, stated (2000 US Dist Lexis 12987 at *15):

> The computer is a piece of tangible personal property. It is operated by mysterious electronic impulses which did not exist when the law of trespass to chattels was developed, but the principles should not be too different. If the electronic impulses can do damage to the computer or to its function in a comparable way to taking a hammer to a piece of machinery, then it is no stretch to recognize that damage as trespass to chattels and provide a legal remedy for it.

To prevail on a claim for trespass to chattels, a plaintiff must prove that the defendant intentionally interfered with the plaintiff's possession of personal property and that the defendant's interference was the proximate cause of the plaintiff's injury. "Where a trespass claim is based on unauthorized access to a computer system, the plaintiff must demonstrate that 1) 'defendant intentionally and without authorization interfered with plaintiff's possessory interest in the computer system; and 2) defendant's unauthorized use proximately resulted in damage to plaintiff.'" *Oyster Software, Inc. v Forms Processing, Inc*. (ND Cal Dec. 6, 2001) 2001 US Dist Lexis 22520 (citations omitted).

Note that consent may bar a claim for trespass to chattels. In *People v Direct Revenue, LLC* (Sup Ct 2008) 862 NYS2d 816, the court rejected the claim that the installation of ad-generating software as part of a bundle of third-party software constituted trespass to chattels. The court concluded that because users of the software had accepted the end-user license agreement authorizing such conduct, their consent barred such a claim.

© The Regents of the University of California

§18.18 1. *eBay Inc. v Bidder's Edge, Inc.*

eBay obtained a preliminary injunction against defendant Bidder's Edge on a trespass to chattels theory in *eBay, Inc. v Bidder's Edge, Inc.* (ND Cal 2000) 100 F Supp 2d 1058. Bidder's Edge operated a website that aggregated information about auctions being conducted on eBay's website through the use of a software robot that "crawled" eBay's site 80,000 to 100,000 times a day. eBay claimed that this activity represented up to 1.53 percent of the total volume of traffic on eBay servers.

eBay sued Bidder's Edge on a number of legal theories, including trespass, false advertising, federal and state trademark dilution, computer fraud and abuse, unfair competition, misappropriation, interference with prospective economic advantage, and unjust enrichment. Citing *CompuServe, Inc. v Cyber Promotions, Inc.* (SD Ohio 1997) 962 F Supp 1015, 1022, the federal district court stated that "[a] trespasser is liable when the trespass diminishes the condition, quality or value of personal property.... The quality or value of personal property may be 'diminished even though it is not physically damaged by defendant's conduct.'" The court found that Bidder's Edge's conduct interfered with eBay's possessory interest in its computer system by "intermeddling with or use of another's personal property."

The court reasoned that even if Bidder's Edge searches used only a small amount of the capacity of eBay's computer systems, Bidder's Edge had nevertheless deprived eBay of the use of that portion of its personal property for its own purposes. Therefore, the actions of Bidder's Edge had caused, and appeared likely to continue to cause, injury to eBay. The court enjoined Bidder's Edge from accessing eBay's computer systems. *eBay, Inc.,* 100 F Supp 2d at 1072.

© The Regents of the University of California

§18.19 2. *Register.com, Inc. v Verio*

The plaintiff in *Register.com, Inc. v Verio, Inc.* (SD NY 2000) 126 F Supp 2d 238, aff'd (2004) 356 F3d 393, operated a domain name registration service. Defendant Verio, Inc. was a provider of web hosting and development services. To market its services to individuals who had recently registered domain names, Verio obtained contact information by using a search robot to comb Register.com's WHOIS database. Verio then used the information collected for mass marketing purposes. Register.com claimed that Verio's activities constituted a trespass to chattels, as well as violations of the Computer Fraud and Abuse Act (18 USC §1030), and the Lanham Act (15 USC §1125(a)), and a breach of the terms of use of its website.

The federal district court found that Verio's use of its search robot exceeded the scope of Register.com's consent, and therefore constituted an unauthorized access. The question remained whether there had been sufficient harm to sustain a trespass claim. The court held that "evidence of mere possessory interference is sufficient to demonstrate the quantum of harm necessary to establish a claim for trespass to chattels." 126 F Supp 2d at 250. The court ruled that Register.com was entitled to a preliminary injunction against Verio on its trespass claim.

© The Regents of the University of California

§18.20 3. *Intel Corp. v Hamidi*

The defendant in *Intel Corp. v Hamidi* (2003) 30 C4th 1342, 71 P3d 296, 1 CR3d 32, a former Intel employee, sent six e-mails criticizing Intel's employment practices over a two-year period to approximately 35,000 Intel employees. The e-mails were sent using Intel's internal e-mail system, but Hamidi did not breach any computer security barriers in transmitting them. He offered to, and did, remove any recipient who wished to be removed from his mailing list. His e-mails did not cause any physical damage or functional disruption to Intel's computers, and did not deprive Intel of the use of its computers. Intel sued Hamidi claiming that his activities constituted a trespass to chattels.

With three out of seven justices dissenting, the California Supreme Court reversed the lower court decisions that had granted Intel's motion for summary judgment. The majority held that (30 C4th at 1347):

> [U]nder California law the tort does not encompass, and should not be extended to encompass, an electronic communication that neither damages the recipient computer system nor impairs its functioning. Such an electronic communication does not constitute an actionable trespass to personal property, i.e., the computer system, because it does not interfere with the possessor's use or possession of, or any other legally protected interest in, the personal property itself.

The court found that Intel had failed to establish a trespass because it failed to present evidence that its computer system sustained injury. See 30 C4th at 1352. In reaching its decision, the court reviewed the leading computer trespass cases, including *eBay, Inc. v Bidder's Edge, Inc.* (ND Cal 2000) 100 F Supp 2d 1058, and *Register.com, Inc. v Verio, Inc.* (SD NY 2000) 126 F Supp 2d 238, aff'd (2004) 356 F3d 393. See §§18.18-18.19. The court found that, in general, in those cases, the defendant's use of the plaintiff's computer system was found sufficient to support an action for trespass to chattels only when it in fact interfered, or threatened to interfere, with the intended functioning of the plaintiff's system, for example, by significantly reducing its available memory or processing power. Intel's case was thus factually distinguishable from the cases involving robots or spammers. *Intel Corp. v Hamidi,* 30 C4th at 1356.

© The Regents of the University of California

§18.20A 4. *Sotelo v DirectRevenue, LLC*

The plaintiff in *Sotelo v DirectRevenue, LLC* (ND Ill 2005) 384 F Supp 2d 1219, filed a putative class action complaint against five defendants, alleging that the defendants caused "spyware" software to be downloaded onto his computer and that the spyware software caused damage to that computer. In ruling on a number of defense motions to dismiss, the court let stand the plaintiff's claim for trespass to chattels, holding that the plaintiff had sufficiently alleged actionable damage caused by the defendants' various advertising-related activities in connection with the spyware at issue.

© The Regents of the University of California

§18.21 5. *Ticketmaster Corp. v Tickets.com, Inc.*

The plaintiff and the defendant in *Ticketmaster Corp. v Tickets.com, Inc*. (CD Cal, Aug. 10, 2000, CV99-7654 HLH) 2000 US Dist Lexis 12987, aff'd without opinion (9th Cir 2001) 248 F3d 1173, were direct business competitors; each operated a commercial website selling tickets to sports and entertainment events. The Tickets.com website described events for which Ticketmaster was the exclusive ticket agent and included a link to Ticketmaster's website to purchase tickets for those events. To obtain the information on the Ticketmaster exclusives, Tickets.com used a "spider" to crawl the Ticketmaster website, extract electronic information posted there, and copy it to its own servers for reformatting and placement on the Tickets.com website. Ticketmaster sued Tickets.com for copyright infringement, unauthorized trespass, and other theories, seeking a preliminary injunction to prevent Tickets.com from continuing to gather information from the Ticketmaster site by use of spiders. The court denied injunctive relief on both the copyright and trespass claims.

On the trespass to chattels claim, the federal district court in a subsequent proceeding held that trespass cannot be established without a showing that "the use or utility of the computer (or computer network) being 'spiderized' is adversely affected by the use of the spider." *Ticketmaster Corp. v Tickets.com, Inc.* (CD Cal, Mar. 7, 2003, CV99-7654 HLH) 2003 US Dist Lexis 6484, *12, aff'd (9th Cir 2005) 127 Fed Appx 346 (unpublished opinion). The court held that a basic element of trespass to chattels is physical harm to the chattel (which the court found not present) or some obstruction of the chattel's basic function (which, in the court's opinion, was not sufficiently shown). Because Tickets.com's spider apparently did not harm Ticketmaster's website, the court granted summary judgment for defendant Tickets.com on the plaintiff's trespass theory. *Ticketmaster Corp. v Tickets.com, Inc., supra*.

The court noted that legal scholars and practitioners have criticized the extension of the tort of trespass to chattels to the Internet context. See, *e.g.,* Quilter, *Cyberlaw: The Continuing Expansion of Cyberspace Trespass to Chattels*, 17 Berkeley Tech L J 421 (2002); *Merrell, Trespass to Chattels in the Age of the Internet*, 80 Wash U L Q 675 (2002). The court stated that the plaintiff must show some tangible interference with the use or operation of the computer being invaded by the spider in order to make out a claim for trespass to chattels. Because Tickets.com's spider did not cause physical injury to the Ticketmaster's computers, Ticketmaster had to show that the use or utility of the computer (or computer network) being "spiderized" was adversely affected by the spider. No such evidence had been presented. The trespass claim was therefore dismissed.

© The Regents of the University of California

§18.21A 6. *Thrifty-Tel, Inc. v Bezenek*

The doctrine of trespass to chattels has also been applied to computer hacking. In *Thrifty-Tel, Inc. v Bezenek* (1996) 46 CA4th 1559, 54 CR2d 468, teenagers hacked into a telephone company's computer system to obtain long distance codes and made long distance phone calls without paying for them. The court found the teenagers liable for trespass to chattels because their "intentional interference with the possession of personal property ha[d] proximately caused injury." 46 CA4th at 1566. The court found that the electronic signals generated by the defendants' activities were sufficiently tangible to support a trespass cause of action. 46 CA4th at 1567 n6.

NOTE: Although the *Bezenek* case involved hacking, it is possible that a court may impose liability under the doctrine of trespass to chattels in the context of unauthorized access to an unsecured wireless network when no hacking occurred. Using another's network arguably causes interference and injury in the form of slower network speeds and reduced network efficiency. However, it is also possible that a court may view the network owner's failure to impose reasonable security measures, such as network access passwords, as an invitation for others to use the network. See §18.7A.

© The Regents of the University of California

III. HOW TO RESPOND TO AN ATTACK

§18.22 A. General Considerations

Cyberattacks usually occur without warning, leaving website operators insufficient time to assess and respond to the situation. The checklist in §18.23 is a general outline of actions to consider if a hacker attack or other network disruption occurs. A major goal of a response plan in a cyberattack should be to preserve evidence for possible use in a later civil or criminal case. Advance planning is crucial to managing the situation and to provide law enforcement with evidence needed to locate the perpetrator. Advance planning can also help a business keep track of the costs associated with the disruption and mitigate its losses. As illustrated by the cases discussed in this chapter, the question of damages is always an important issue. An affected business should document carefully all associated expenses or losses in anticipation of the need to prove damages at trial.

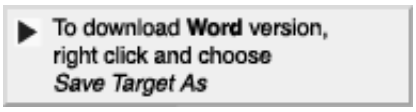
Federal agencies have reorganized in an effort to protect the Internet infrastructure from potential terrorist attacks. In 2003, the Department of Homeland Security (DHS) partnered with the private sector to form US-CERT (Computer Emergency Readiness Team), the operational arm of the National Cyber Security Division at DHS. The purpose of US-CERT is to act as a clearinghouse for up-to-date computer security information through the National Cyber Alert System and its website at http://www.us-cert.gov.

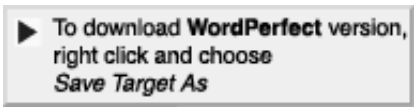
Victims of cyber crimes should consider filing a complaint with the Internet Crime Complaint Center (IC3), a partnership among the FBI, National White Collar Crime Center, and the Bureau of Justice Assistance. The IC3 website also provides Internet crime prevention tips and current trends in Internet crime schemes. See http://www.ic3.gov/default.aspx.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/18 Viruses and Other Network Disruptions/§18.23 B. Checklist: Responding to a Cyberattack

§18.23 B. Checklist: Responding to a Cyberattack





1. Contact

- Legal counsel.
- Local law enforcement.
- US-CERT encourages the private sector to report security breaches and other service disruptions to http://www.us-cert.gov. The website uses a secure sockets layer (SSL), and no confidential system information is released without authorization.
- Any applicable insurance carriers.
- Website host or Internet service provider (ISP). The ISP or website host may be able to help identify the Internet protocol (IP) address from which the intruder accessed the website and help identify the areas of the site that may be compromised.
- If unencrypted personal information is maintained on the website, comply with CC §1798.82 and notify the persons affected.

2. Assess damage

- Determine if the attack physically damaged any hard drives or electronic files.
- List and isolate every electronic file taken or destroyed.
- Assemble evidence, including any evidence that the attack compromised trade secrets or confidential proprietary information of the company, its customers, or its employees. If financial information such as credit card data has been accessed, inform officials at the company's authorizing bank.
- Document network downtime and impairment of service availability to customers.

3. Keep track of costs

- Keep a log of all remedial work undertaken, including the number of hours and costs and expenses.
- Keep track of expenses incurred as a result of the attack, including the cost of hiring third party consultants, loss of productivity, lost profits, and hardware and software costs.
- Evaluate the cost of recovering or recreating lost data.

4. Preserve evidence

- Isolate the computer or server accessed, which may have sustained damage, in a secure location to preserve any clues to the intruder's identity. It is important not to lose or compromise any data that might provide information as to the identity of the intruder.
- Shut down or reconfigure the system if possible so that it does not run utility programs automatically. Automated maintenance or utility programs can delete and recycle data on a hard drive, and potentially destroy evidence automatically. Consider engaging an expert to review the system's status and preserve electronic copies of the evidence on a separate system.
- Preserve the state of the computer or server by backing up the hard drive and storing the backups in a secure location. Do not write over existing backup files because they may constitute evidence of the system's status before the attack and may be the only way to retrieve critical data.
- To the extent possible, avoid attempting to remediate the damage caused to individual computers and systems until law enforcement can collect evidence.
- Obtain any relevant network access logs.

- Interview current employees to determine if any of them have evidence pertinent to the identity of the perpetrator. Many attacks are made by disgruntled employees or others known to the target company.
- Disconnect the computer or server from the Internet as soon as it is known that security has been compromised. Hackers may monitor the affected systems and erase their trails or the company's attempts to preserve hackers' trails. Take the website offline to prevent further damage, and post a notice in place of the company's home page to inform visitors that the site is temporarily unavailable.
- Print hard copies of key information if possible. Hard copies cannot be modified by hackers.

© The Regents of the University of California

19

Jurisdiction; Conflicts of Law

I. INTERNET JURISDICTION
- A. Introduction §19.1
- B. Personal Jurisdiction §19.2
  - 1. State Long-Arm Statutes §19.3
  - 2. Federal Rules of Civil Procedure §19.4
  - 3. Constitutional Limits on Personal Jurisdiction
    - a. Due Process Clause §19.5
    - b. Minimum Contacts Test §19.6
    - c. Reasonableness §19.7
  - 4. General and Specific Personal Jurisdiction
    - a. General Personal Jurisdiction §19.8
    - b. Specific Personal Jurisdiction §19.9
    - c. Specific Jurisdiction in Cyberspace §19.10
- C. In Rem Jurisdiction; Anticybersquatting Consumer Protection Act §19.11
- D. Choice-of-Forum Clauses
  - 1. Enforceability §19.12
  - 2. Form: Choice-of-Forum Clause §19.13

II. CONFLICTS OF LAW; CHOICE-OF-LAW CLAUSES
- A. Conflicts of Law
  - 1. Generally §19.14
  - 2. Constitutional Analysis §19.15
  - 3. Is There a Choice-of-Law Clause? §19.16
  - 4. Governmental Interest Analysis §19.17
  - 5. Conflicts of Law on Internet §19.18
- B. Choice-of-Law Clauses
  - 1. Enforceability
    - a. California Statutes §19.19
    - b. *Nedlloyd Lines, B.V. v Superior Court* and Later Cases §19.20
  - 2. Drafting Considerations §19.21
  - 3. Form: Choice-of-Law Clause §19.22

© The Regents of the University of California

I. INTERNET JURISDICTION

§19.1 A. Introduction

Jurisdiction is the power of the court to which a case is presented to assert authority over the persons or things involved in the action and to decide the case or issue a decree relating to it. The concept encompasses both personal jurisdiction (also referred to as in personam jurisdiction) and subject matter jurisdiction. A court must have personal jurisdiction to exercise its authority over the parties to an action. Generally, courts use a "minimum contacts" test to determine whether personal jurisdiction obtains over a defendant. See *International Shoe Co. v Washington* (1945) 326 US 310, 90 L Ed 95, 66 S Ct 154; *Boschetto v Hansing* (9th Cir 2008) 539 F3d 1011; *Pebble Beach Co. v Caddy* (9th Cir 2006) 453 F3d 1151; §§19.5-19.7. With the growth of the Internet, courts have fashioned a passive-active online interaction test to evaluate minimum contacts in cyberspace. See *Cybersell, Inc. v Cybersell, Inc.* (9th Cir 1997) 130 F3d 414; *Zippo Mfg. v Zippo Dot Com* (WD Pa 1997) 952 F Supp 1119 (discussed in §19.10).

In rem jurisdiction is analogous to personal jurisdiction, but it constitutes jurisdiction over specific property, not human beings. In exercising in rem jurisdiction, the court determines rights with respect to a particular item of property, such as a domain name. See §19.11.

Subject matter jurisdiction concerns the court's authority over the case itself and the type of relief sought. The subject matter jurisdiction of the federal courts in both civil and criminal cases is limited to the matters specified in Article III, §2 of the U.S. Constitution and in federal statutes. Very generally, there are two main types of federal subject matter jurisdiction in civil cases: (1) federal question jurisdiction, *i.e.,* cases arising under the United States Constitution or under federal statutes such as the Digital Millennium Copyright Act (Pub L 105-304, 112 Stat 2860; 28 USC §1331) (see §1.24), and (2) diversity jurisdiction, *i.e.,* cases between citizens of different states in which the amount in controversy exceeds $75,000 (28 USC §1332). Unlike the federal courts, the subject matter jurisdiction of the state courts is not limited. State courts have general subject matter jurisdiction over any matter that is not the exclusive province of the federal courts.

© The Regents of the University of California

§19.2 B. Personal Jurisdiction

A court's authority to exercise personal jurisdiction over a litigant derives from the jurisdictional statutes of the state in which the court sits. *Zippo Mfg. v Zippo Dot Com* (WD Pa 1997) 952 F Supp 1119, 1122. As a general rule, personal jurisdiction over a defendant is proper if permitted by the state's long-arm statute (see, *e.g.,* CCP §410.10) and if the court's exercise of jurisdiction comports with the limits established by the due process clause of the United States Constitution. *Boschetto v Hansing* (9th Cir 2008) 539 F3d 1011; *Pebble Beach Co. v Caddy* (9th Cir 2006) 453 F3d 1151. Issues of personal jurisdiction may arise in cases involving defendants who are not residents of the state in which the action is commenced.

Personal jurisdiction is an issue in much Internet-related litigation because of the global reach of the medium. Interpreting Fed R Civ P 4(f), which governs service on individuals outside of United States jurisdiction, the Ninth Circuit acknowledged changes in technology and held that e-mail service was appropriate as the method most likely to apprise the defendant that an action was pending. *Rio Props., Inc. v Rio Int'l Interlink* (9th Cir 2002) 284 F3d 1007, 1017. See also *Williams-Sonoma, Inc. v FriendFinder, Inc.* (ND Cal, April 17, 2007, No. C 06-06572 JSW) 2007 US Dist Lexis 31299 (e-mail service on allegedly infringing foreign website operators permitted).

© The Regents of the University of California

§19.3 1. State Long-Arm Statutes

All states have long-arm statutes that determine the limits within which their courts may exercise personal jurisdiction over nonresident litigants. California's long-arm statute provides that a court may exercise jurisdiction over a defendant on any basis not inconsistent with the constitution of California or the United States. CCP §410.10. This long-arm statute, like many enacted by other states, allows California courts to assert jurisdiction to the limits of due process under the Fifth and Fourteenth Amendments of the United States Constitution. Not all states, however, authorize their courts to exercise jurisdiction to the extent permitted by due process. See, *e.g., Bensusan Restaurant Corp. v King* (2d Cir 1997) 126 F3d 25 (court may not exercise personal jurisdiction over nonresident defendant under New York's long-arm statute unless nonresident defendant expects or should have expected tortious act to have consequences in New York and unless defendant derives substantial revenue from interstate commerce). See also *Goldhaber v Kohlenberg* (NJ Super 2007) 928 A2d 948 (New Jersey courts have jurisdiction over California defendant who targeted New Jersey plaintiffs with defamatory messages).

© The Regents of the University of California

§19.4 2. Federal Rules of Civil Procedure

Under the Federal Rules of Civil Procedure, federal courts may exercise personal (or in rem) jurisdiction pursuant to the law of the state in which the court sits. Fed R Civ P 4(e). Thus, a federal court sitting in California looks to California law to determine its authority to exercise personal jurisdiction over a nonresident defendant.

In certain cases involving defendants outside the United States, Fed R Civ P 4(k)(2) may also serve as a basis for establishing personal jurisdiction. See *Pebble Beach Co. v Caddy* (9th Cir 2006) 453 F3d 1151. This rule provides that in federal question cases (see §19.1), a federal court may obtain personal jurisdiction over a defendant if the defendant is not subject to jurisdiction in any state court and the court's exercise of jurisdiction is consistent with the U.S. Constitution and U.S. law.

© The Regents of the University of California

3. Constitutional Limits on Personal Jurisdiction

§19.5 a. Due Process Clause

Courts may not exercise jurisdiction outside the boundaries set by the due process clause of the Constitution. Early cases held that personal jurisdiction over a litigant could obtain on three bases: (1) a person's presence in the jurisdiction (*Pennoyer v Neff* (1878) 95 US (5 Otto) 714 (upholding exercise of personal jurisdiction based upon service of process delivered in forum state); see also *Burnham v Superior Court* (1990) 495 US 604, 109 L Ed 2d 631, 110 S Ct 2105); (2) a person's residence or domicile in the state (*Milliken v Meyer* (1940) 311 US 457, 85 L Ed 278, 61 S Ct 339); or (3) consent to the court's jurisdiction (often achieved through contractual forum selection clauses; see §§19.12-19.13).

International Shoe Co. v Washington (1945) 326 US 310, 90 L Ed 95, 66 S Ct 154, ushered in the modern due process approach based on fairness, which essentially expanded the courts' power to exercise jurisdiction over nonresident litigants. *International Shoe* held that personal jurisdiction may be exercised when the litigant has sufficient minimum contacts with the forum state such that the maintenance of the suit against the defendant does not offend "traditional notions of fair play and substantial justice." 326 US at 316, 90 L Ed at 102 (citing *Milliken v Meyer* (1940) 311 US 457, 463, 85 L Ed 278, 283, 61 S Ct 339). To determine whether this requirement has been met, a court analyzes two factors: the scope of contacts with the forum state and, when necessary, the reasonableness of pursuing a case in that forum. *Burger King v Rudzewicz* (1985) 471 US 462, 85 L Ed 2d 528, 105 S Ct 2174.

© The Regents of the University of California

§19.6 b. Minimum Contacts Test

To determine whether contacts are sufficient to satisfy due process, the court will look at the quantity and nature of the defendant's contacts with the forum, the nexus between the contacts and the cause of action, and the interest of the forum in protecting its citizens. *Shaffer v Heitner* (1977) 433 US 186, 53 L Ed 2d 683, 97 S Ct 2569. A defendant that avails itself of the privilege of conducting business in the forum and whose activities are shielded by "the benefits and protections" of the forum state's laws may reasonably expect to be subjected to litigation there. *Burger King v Rudzewicz* (1985) 471 US 462, 476, 85 L Ed 2d 528, 543, 105 S Ct 2174; *Keeton v Hustler Magazine, Inc.* (1984) 465 US 770, 79 L Ed 2d 790, 104 S Ct 1473 (defendant purposefully availed itself of opportunity to engage in in-state activities by distributing magazine in state); *World-Wide Volkswagen v Woodson* (1980) 444 US 286, 62 L Ed 2d 490, 100 S Ct 559 (car dealer that did not advertise, sell cars, or deliberately target or cultivate customers in forum state did not purposefully avail itself of opportunity to conduct business in state, although it was foreseeable that customers would take its cars there). Contacts must be substantial enough to put the defendant on notice that it may be subject to personal jurisdiction in that forum; otherwise, exercise of jurisdiction may offend traditional notions of fair play and substantial justice. *International Shoe Co. v Washington* (1945) 326 US 310, 316, 90 L Ed 95, 102, 66 S Ct 154.

In *Boschetto v Hansing* (9th Cir 2008) 539 F3d 1011, the Ninth Circuit held that a California resident's purchase of a car from a resident of another state via an Internet auction site did not provide sufficient minimum contacts to enable a California court to exercise jurisdiction over the seller. By making only a single sale from his home state—a "one-shot affair"—the seller did not purposefully avail himself of the privilege of doing business in California. 539 F3d at 1017. The single-sale transaction was too limited to create the requisite substantial connection needed to establish jurisdiction. The court noted, however, that when a defendant is "using the platform as a broader vehicle for commercial activity," jurisdiction based on Internet sales may be proper. 539 F3d 1019.

© The Regents of the University of California

§19.7 c. Reasonableness

Minimum contacts alone are not sufficient to satisfy due process. The exercise of jurisdiction must be reasonable in order to protect defendants against unfairly inconvenient litigation. *Zippo Mfg. v Zippo Dot Com* (WD Pa 1997) 952 F Supp 1119, 1123 (citing *World-Wide Volkswagen v Woodson* (1980) 444 US 286, 62 L Ed 2d 490, 100 S Ct 559). See also *Asahi Metal Indus. Co. v Superior Court* (1987) 480 US 102, 94 L Ed 2d 92, 107 S Ct 1026 (unreasonable to subject tire manufacturer to jurisdiction in every state in which tires might be used). To assess reasonableness, the court balances several factors (*Panavision Int'l v Toeppen* (9th Cir 1998) 141 F3d 1316, 1323):

> (1) the extent of a defendant's purposeful interjection; (2) the burden on the defendant in defending in the forum; (3) the extent of conflict with the sovereignty of the defendant's state; (4) the forum state's interest in adjudicating the dispute; (5) the most efficient judicial resolution of the controversy; (6) the importance of the forum to the plaintiff's interest in convenient and effective relief; and (7) the existence of an alternative forum.

Once the court finds that the defendant purposefully directed its activities to the forum state, the burden is on the defendant to show that exercise of jurisdiction is unreasonable. 141 F3d at 1323.

© The Regents of the University of California

4. General and Specific Personal Jurisdiction

§19.8 a. General Personal Jurisdiction

A court may exercise general personal jurisdiction over a defendant for any cause of action under the traditional bases of presence, domicile, or consent, or when the defendant's contacts with the forum state have been substantial or sufficiently continuous and systematic to justify a suit. *International Shoe Co. v Washington* (1945) 326 US 310, 90 L Ed 95, 66 S Ct 154. The asserted cause of action need not be related to the defendant's activities in the forum.

Many online businesses lack a traditional physical headquarters in a single jurisdiction and routinely market their products or services globally. Courts addressing Internet-related disputes have therefore evolved additional criteria with which to evaluate jurisdiction. See, *e.g., Gorman v Ameritrade Holding Corp.* (DC Cir 2002) 293 F3d 506, 516 (Nebraska defendant whose highly interactive web site allowed Washington, D.C., users to manipulate brokerage accounts was "quite wrong in treating 'cyberspace' as if it were a kingdom floating in the mysterious ether, immune from the jurisdiction of earthly courts"). The standard for general personal jurisdiction is "fairly high"; a defendant's contacts with the forum must "be of the sort that approximate physical presence." *Bancroft & Masters, Inc. v Augusta Nat'l, Inc*. (9th Cir 2000) 223 F3d 1082, 1086 (Georgia defendant's "passive" website and occasional unsolicited sales to California residents not sufficient to establish general jurisdiction). See also *Metro-Goldwyn-Mayer Studios, Inc. v Grokster, Ltd.* (CD Cal 2003) 243 F Supp 2d 1073 (providing software to two million California residents, using California public relations firms and law firms as agents, and assuming contracts with California companies do not approximate physical presence, but because defendant's significant commercial contacts gave rise to plaintiff's cause of action, specific jurisdiction was proper).

In 2005, the California Supreme Court held that several defendants who operated hotels in Nevada were properly subject to California jurisdiction based on the group's advertising activities on its Internet website. *Snowney v Harrah's Entertainment, Inc.* (2005) 35 C4th 1054, 29 CR3d 33 (defendants purposefully availed themselves of privilege of doing business in California by advertising proximity of their resorts to California and enabling California residents to reserve rooms via their interactive website). The court focused on the fact that the defendants' website specifically targeted residents of California by, *e.g*., providing driving directions from California and including statements about the proximity of its hotels to California. Further, many customers coming from California made reservations using the website. Although the defendants also engaged in activities unrelated to the Internet, such as an extensive California advertising campaign and direct mailings to California residents, the court stated, "We need not… decide on a particular approach here because defendants' Web site, by any standard, establishes purposeful availment [of the privilege of conducting business in California].… [D]efendants' site specifically targeted residents of California." 35 C4th at 1064.

© The Regents of the University of California

§19.9 b. Specific Personal Jurisdiction

When general jurisdiction over a nonresident based on presence, domicile, consent, or substantial or continuous and systematic contacts cannot be found, specific jurisdiction may exist for a particular claim arising out of the defendant's actions within the forum state. In the Ninth Circuit, federal courts apply a three-part test to determine whether the exercise of specific jurisdiction over a nonresident defendant is appropriate (*Boschetto v Hansing* (9th Cir 2008) 539 F3d 1011, 1016):

> (1) The non-resident defendant must purposefully direct his activities or consummate some transaction with the forum or resident thereof; or perform (some act by which he purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections of its laws;
> (2) the claim must be one which arises out of or relates to the defendant's forum-related activities; and
> (3) the exercise of jurisdiction must comport with fair play and substantial justice, i.e. it must be reasonable.

See also *Pebble Beach Co. v Caddy* (9th Cir 2006) 453 F3d 1151; *Cybersell, Inc. v Cybersell, Inc.* (9th Cir 1997) 130 F3d 414.

Courts have considered a variety of factors in determining whether specific personal jurisdiction exists:

- Local phone numbers, as distinct from toll free numbers, indicate the restricted scope of the intended audience, tending to rule out a finding of specific jurisdiction elsewhere. *Cybersell, Inc. v Cybersell, Inc.* (9th Cir 1997) 130 F3d 414.
- Conducting business with or soliciting business from forum residents tends to support a finding of specific jurisdiction in that forum. *CompuServe, Inc. v Patterson* (6th Cir 1996) 89 F3d 1257. See also *Metro-Goldwyn-Mayer Studios, Inc. v Grokster, Ltd.* (CD Cal 2003) 243 F Supp 2d 1073. But see *Millennium Enters., Inc. v Millennium Music LP* (D Or 1999) 33 F Supp 2d 907, 921 (defendants' website, although interactive, published information "accessible to whomever may find it"; it did not operate to provide defendants with "fair warning" that they could anticipate being hauled into court anywhere).
- Directing e-mail, telephone calls, faxes, and letters to the forum state favors a finding of personal jurisdiction there. *Hall v LaRonde* (1997) 56 CA4th 1342, 1347, 66 CR2d 399 ("The speed and ease of [electronic] communications have increased the number of transactions that are consummated without either party leaving the office. There is no reason why the requisite minimum contacts cannot be electronic").
- Intentionally tortious conduct may subject the actor to personal jurisdiction in the state where the action had an injurious effect (the effects doctrine). *Panavision Int'l v Toeppen* (9th Cir 1998) 141 F3d 1316, 1321 (Illinois-based cybersquatter subject to California jurisdiction when he registered as domain names trademarks of corporation with its principal place of business in California).
- Willfully infringing a copyright owned by a resident of the forum, with knowledge that the plaintiff's principal place of business is in that forum, is sufficient to establish personal jurisdiction there. *Columbia Pictures Television v Krypton Broad. of Birmingham, Inc.* (9th Cir 1997) 106 F3d 284, rev'd on other grounds sub nom *Feltner v Columbia Pictures Television* (1998) 523 US 340.
- Sending defamatory e-mails into Texas established personal jurisdiction in Texas over a California resident. *Middlebrook v Anderson* (ND Tex, Feb. 11, 2005, No. 3:04-CV-2294-D) 2005 US Dist Lexis 1976.
- Making a single sale in the jurisdiction, along with e-mail and instant messenger contact, was sufficient to establish jurisdiction over the defendant in a New York court in a domain name dispute (the fact that the sale was to the plaintiff's investigator was irrelevant). *Mattel, Inc. v Procount Bus. Serv.* (SD NY, Mar. 10, 2004, No. 03 Civ 7234 (RWS)) 2004 US Dist Lexis 3895.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/19 Jurisdiction; Conflicts of Law/§19.10 c. Specific Jurisdiction in Cyberspace

§19.10 c. Specific Jurisdiction in Cyberspace

Specific personal jurisdiction over persons transacting business or communicating over the Internet has been the subject of much debate. The Supreme Court has yet to rule on the question, and in early 2003, it denied certiorari on a case that addressed the issue. See *ALS Scan, Inc. v Digital Serv. Consultants* (4th Cir 2002) 293 F3d 707, cert denied (2003) 537 US 1105 (Maryland lacked jurisdiction over Georgia Internet service provider whose customer allegedly violated Maryland copyright laws).

Internet jurisdiction cases indicate that the fundamental test requiring minimum contacts for specific personal jurisdiction set forth in *International Shoe Co. v Washington* (1945) 326 US 310, 318, 90 L Ed 95, 103, 66 S Ct 154, still applies. In cyberspace, "the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet." *Zippo Mfg. v Zippo Dot Com* (WD Pa 1997) 952 F Supp 1119, 1124. The *Zippo* court utilized a "sliding scale" of electronic contacts on which the likelihood of the exercise of personal jurisdiction over that defendant is based (952 F Supp at 1124):

> At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper [citation omitted]. At the opposite end are situations where a defendant has simply posted information on an Internet web site which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise of personal jurisdiction [citation omitted]. The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer.

The court found that the defendant's activity in the forum—selling passwords to 3000 Pennsylvania subscribers and signing seven contracts with Internet providers to provide its services to Pennsylvania—constituted "purposeful availment of doing business [in the state]." 952 F Supp at 1126. In addition, the court found that the use of the website by the Pennsylvania residents was not "fortuitous" within the meaning of *World-Wide Volkswagen v Woodson* (1980) 444 US 286, 62 L Ed 2d 490, 100 S Ct 559, in which the plaintiffs were injured in Oklahoma after they drove a car bought in New York into that state and subsequently tried to sue the car dealer there. 952 F Supp at 1126. See also *Carefirst of Maryland, Inc. v Carefirst Pregnancy Ctrs., Inc.* (4th Cir 2002) 305 F3d 253 (owner of "semi-interactive" websites asserting commitment to Chicago area women not subject to Maryland jurisdiction because sites were not directed to Maryland consumers).

PRACTICE TIP: Website operators should be made aware that jurisdiction is not based solely on transactions involving sales of goods, but also on other functionality that can be characterized as "exchange of information." If a site permits users to request subscriptions to e-mailed newsletters or to e-mail the site directly with questions or requests, those features may be deemed sufficient to characterize the site as an "interactive" site under the *Zippo* standard. *Blumenthal v Drudge* (D DC 1998) 992 F Supp 44.

In *Boschetto v Hansing* (9th Cir 2008) 539 F3d 1011, the Ninth Circuit held that a California resident's purchase of a car from a resident of another state via an Internet auction site did not provide sufficient minimum contacts to enable a California court to exercise jurisdiction over the seller. By making only a single sale from his home state—a "one-shot affair"—the seller did not purposefully avail himself of the privilege of doing business in California. 539 F3d at 1017. The single-sale transaction was too limited to create the requisite substantial connection needed to establish jurisdiction. The court noted, however, that when a defendant is "using the platform as a broader vehicle for commercial activity," jurisdiction based on Internet sales may be proper. 539 F3d 1019. See also *Shisler v Sanfer Sports Cars, Inc.* (2006) 146 CA4th 1254, 1261, 53 CR3d 335 (sale of defective automobile advertised online by Florida company to California resident was one-time transaction insufficient to establish personal jurisdiction).

In *Pebble Beach Co. v Caddy* (9th Cir 2006) 453 F3d 1151, the Ninth Circuit Court of Appeals found that the combination of a domain name that refers to a geographic location in California, a ".com" suffix, and a noninteractive, passive website is inadequate to establish personal jurisdiction in California. Caddy, owner of the Pebble Beach Bed &

Breakfast in England, operates a website located at http://www.pebblebeach-uk.com. The website includes information about the bed and breakfast and does not have an online reservation system or online inquiry forms. Pebble Beach Company owns a golf course resort in California and operates the http://www.pebblebeach.com website. 453 F3d 1153. The Pebble Beach Company sued Caddy for infringement and dilution of its "Pebble Beach" trademark. The court found that Caddy's actions, operating its passive website to market a legitimate establishment using the "Pebble Beach" name, were not expressly aimed at California. 453 F3d at 1157. The court held, "The fact that the name 'Pebble Beach' is a famous mark known world-wide is of little practical consequence when deciding whether action is directed at a particular forum via the world wide web." The court also found Caddy's selection of a ".com" domain name instead of a United Kingdom or European Union domain name "of little importance." 453 F3d at 1159.

PRACTICE TIP: Companies doing business online should be aware that website transactions are not the only factors relevant in determining whether a court would have personal jurisdiction over them. For example, a court will have personal jurisdiction over a company that is incorporated or maintains its principal place of business in the state where the court sits, based on domicile.

Personal jurisdiction in international cases, including a review of *Yahoo!, Inc. v La Ligue Contre le Racisme et L'Antisemitisme* (9th Cir 2004) 379 F3d 1120, rehearing en banc granted (Feb. 10, 2005, No. 01-17424) 399 F3d 1010, is discussed in §21.5.

© The Regents of the University of California

§19.11 C. In Rem Jurisdiction; Anticybersquatting Consumer Protection Act

In rem jurisdiction is the exercise of jurisdiction over specific property located in the forum state. In rem jurisdiction is often used to adjudicate property rights when the owners of the property are unknown or the property is in dispute. Traditionally, exercise of in rem jurisdiction has been limited to tangible property. This limitation has presented special problems for plaintiffs in Internet-related cases seeking to protect intellectual property, such as a domain name. The Anticybersquatting Consumer Protection Act (ACPA) (Pub L 106-113, 113 Stat 1501A, principally codified at 15 USC §1125(d)) helps protect owners of trade names and trademarks by giving them a remedy against persons or entities using a mark identical or confusingly similar to their own with bad faith intent to profit from the mark. The ACPA represents a significant step beyond the Trademark Dilution Act (Pub L 104-98, 109 Stat 985) (see §§3.22-3.25), because it allows owners of intangible property, *i.e.,* domain names, to make use of in rem jurisdiction to settle rights to the use of the name. 15 USC §1125(d). In rem jurisdiction is available only if the owner of a protected mark is unable to obtain personal jurisdiction over the would-be defendant. 15 USC §1125(d)(2). If personal jurisdiction is unavailable, the ACPA allows the court to exercise in rem jurisdiction over the domain name itself, which is deemed the defendant in the case, to determine whether the domain name infringes the plaintiff's mark. See *Porsche Cars N.A., Inc. v Porsche.net* (4th Cir 2002) 302 F3d 248 (despite Congressional preference for personal jurisdiction, defendant's last-minute decision to submit to personal jurisdiction in California did not defeat exercise of in rem jurisdiction in pending Virginia action).

© The Regents of the University of California

D. Choice-of-Forum Clauses

§19.12 1. Enforceability

Choice-of-forum clauses in contracts express the parties' agreement regarding which court, sitting in which city, state, or country, will handle any dispute relating to the contract between the parties. The Supreme Court has held that a choice-of-forum clause in a freely negotiated contract will be upheld unless it is unreasonable, unjust, or invalid because of fraud, or it contravenes strong public policy of the forum where the suit was brought. See *Carnival Cruise Lines, Inc. v Shute* (1991) 499 US 585, 592, 113 L Ed 2d 622, 632, 111 S Ct 1522 (choice-of-forum clause in standard cruise ship ticket upheld because it provides certainty regarding where suits arising from contract may be brought); *M/S Bremen v Zapata Off-Shore Co.* (1972) 407 US 1, 32 L Ed 2d 513, 92 S Ct 1907 (enforcement of choice-of-forum clause in shipping contract negotiated at arm's length not unreasonable); *Argueta v Banco Mexicano* (9th Cir 1996) 87 F3d 320, 324 (choice of forum clause enforceable unless there is evidence establishing "fraud, undue influence, overweening bargaining power, or such serious inconvenience in litigating in the selected forum so as to deprive that party of a meaningful day in court").

The leading California case is *Smith, Valentino & Smith, Inc. v Superior Court* (1976) 17 C3d 491, 495, 131 CR 374, in which the court stated:

> While it is true that the parties may not *deprive* courts of their jurisdiction over causes by private agreement… courts possess discretion to *decline* to exercise jurisdiction in recognition of the parties' free and voluntary choice of a different forum.… [A]lthough we have acknowledged a policy favoring access to California courts by resident plaintiffs… the policy is satisfied in those cases where, as here, a plaintiff has freely and voluntarily negotiated away his right to a California forum. In so holding we are in accord with the modern trend which favors enforceability of such forum selection clauses. [Citations omitted; emphasis in original.]

If a lawsuit is commenced in a forum other than the one selected by the parties to the contract and the choice-of-forum clause is enforced, the suit will be subject to dismissal for improper venue. See *Carnival Cruise Lines, Inc. v Shute, supra*.

The public policy exception to enforceability of forum selection clauses was successfully invoked in *America Online, Inc. v Superior Court* (2001) 90 CA4th 1, 108 CR2d 699, a consumer class-action lawsuit. At issue was a clause in AOL's online terms of service agreement designating the courts of Virginia as the exclusive forum for resolution of any claim or dispute concerning AOL's services. Noting that Virginia law did not permit consumer lawsuits to be brought as class actions and that plaintiffs' remedies were more limited there, the court found that the plaintiffs' rights would be substantially diminished if they were forced to litigate in Virginia. The forum selection clause violated important public policy underlying California's consumer protection laws. Accordingly, it was not enforceable. See also *America Online, Inc. v Pasieka* (Fla App 2004) 870 So2d 170.

Choice-of-forum clauses can be exclusive or nonexclusive. Exclusive clauses make the selected forum mandatory for all litigation; nonexclusive clauses merely state that the parties would agree to jurisdiction in that state without binding them to bring their claims there and nowhere else. *Koresko v RealNetworks, Inc*. (ED Cal 2003) 291 F Supp 2d 1157 (clearly worded exclusive forum selection clause enforceable; no hardship for California resident to litigate in Washington forum selected by contract).

PRACTICE TIP: A clause that is intended to be exclusive should include the word "exclusive" or a similar term. Otherwise, it may be deemed permissive rather than mandatory. See *Koresko v RealNetworks, Inc*., *supra*; *Thompson v Handa-Lopez* (WD Tex 1998) 998 F Supp 738.

Reciprocal clauses, in which the parties agree that the forum will be the state of the defendant, can also serve to deter litigation if the contracting parties are located in jurisdictions distant from one another.

The California Code of Civil Procedure includes a provision assuring the enforceability of choice-of-forum clauses in contract cases involving transactions of $1 million or more that the parties have chosen to be governed by California

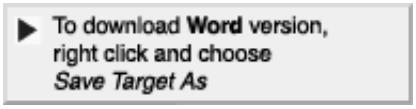
law (CCP §410.40):

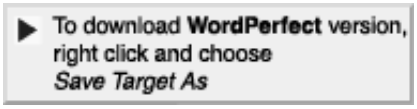
> Any person may maintain an action or proceeding in a court of this state against a foreign corporation or nonresident person where the action or proceeding arises out of or relates to any contract, agreement, or undertaking for which a choice of California law has been made in whole or in part by the parties thereto and which (a) is a contract, agreement, or undertaking, contingent or otherwise, relating to a transaction involving in the aggregate not less than one million dollars ($1,000,000), and (b) contains a provision or provisions under which the foreign corporation or nonresident agrees to submit to the jurisdiction of the courts of this state.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/19 Jurisdiction; Conflicts of Law/§19.13 2. Form: Choice-of-Forum Clause

§19.13 2. Form: Choice-of-Forum Clause





CHOICE OF FORUM. Any dispute arising out of this Agreement (whether contract, tort, or both) shall be submitted to a state or federal court sitting in _ _[*city or county, state, e.g., Los Angeles, California*]_ _, which will have exclusive jurisdiction over the dispute and to which jurisdiction the parties irrevocably submit.

© The Regents of the University of California

II. CONFLICTS OF LAW; CHOICE-OF-LAW CLAUSES

A. Conflicts of Law

§19.14 1. Generally

Litigation involving parties from different jurisdictions or events occurring in different jurisdictions often results in conflicts over which jurisdiction's laws should be applied to resolve the case. In the United States, conflicts-of-law determinations depend on state statutes and case law applied within the boundaries of the United States Constitution. Which state's law is applied in a particular case may affect issues from the plaintiff's right to sue through the procedures for enforcement of the plaintiff's judgment.

© The Regents of the University of California

§19.15 2. Constitutional Analysis

The Due Process and Full Faith and Credit clauses of the United States Constitution set important boundaries in conflicts-of-law analysis, although constitutional requirements are usually met if the court has personal jurisdiction over the parties. The leading case on the constitutional aspects of conflicts-of-law analysis is *Allstate Ins. Co. v Hague* (1981) 449 US 302, 66 L Ed 2d 521, 101 S Ct 633. *Allstate* indicates that the purpose of the constitutional analysis in conflicts disputes is not to determine which law should govern a conflict but rather to ensure that the choice of a particular body of substantive law does not exceed federal constitutional limitations. 449 US at 307, 66 L Ed 2d at 527. For a state's substantive law to be applied in a constitutionally permissible manner, that state must have a significant contact or a significant aggregation of contacts creating state interests, such that application of that state's law is neither arbitrary nor fundamentally unfair. 449 US at 312, 66 L Ed 2d at 530. See also *Phillips Petroleum Co. v Shutts* (1985) 472 US 797, 818, 86 L Ed 2d 628, 105 S Ct 2965.

The constitutional aspect of conflicts-of-law analysis is very similar to the determination of personal jurisdiction: both are based on the Due Process clause of the Fourteenth Amendment. In deciding constitutional conflicts-of-law issues, the Supreme Court examines the contacts of the state whose law was applied with the parties and with the occurrence or transaction giving rise to the litigation, as is done in personal jurisdiction analysis. 449 US at 308, 328 (citing *Clay v Sun Ins. Office, Ltd.* (1964) 377 US 179, 183, 12 L Ed 2d 229, 232, 84 S Ct 1197). As a result, a finding on personal jurisdiction is significant, although not conclusive, in reviewing the constitutionality of the use of the forum state's substantive law.

© The Regents of the University of California

§19.16 3. Is There a Choice-of-Law Clause?

In contract disputes, conflicts-of-law determinations depend on whether the contract has a choice-of-law clause. The enforceability of choice-of-law clauses is discussed in §§19.19-19.22. For contracts lacking choice-of-law clauses, CC §1646 provides:

> A contract is to be interpreted according to the law and usage of the place where it is to be performed; or, if it does not indicate a place of performance, according to the law and usage of the place where it is made.

The continued force of CC §1646 is questionable, however, in light of the California Supreme Court precedent that requires conflicts-of-law issues in contract cases not involving choice-of-law clauses (as well as in tort cases) to be resolved under a "governmental interest" approach. See *Washington Mut. Bank, FA v Superior Court* (2001) 24 C4th 906, 919, 103 CR2d 320; §19.17.

© The Regents of the University of California

§19.17 4. Governmental Interest Analysis

Even when California law may constitutionally be applied (see §19.15), California courts utilize a three-step "governmental interest" analysis to resolve conflicts-of-law issues and determine the most appropriate law to be applied in the absence of an effective choice-of-law agreement. *Washington Mut. Bank, FA v Superior Court* (2001) 24 C4th 906, 919, 103 CR2d 320. The "governmental interest" approach is followed both in tort cases (see, *e.g., Offshore Rental Co. v Continental Oil Co.* (1978) 22 C3d 157, 148 CR 867) and in contracts cases where the contract lacks a choice-of-law clause (see, *e.g., Washington Mut. Bank, FA v Superior Court, supra*).

Under the "governmental interest" analysis, the court will apply California law unless a litigant asserts that the law of another forum should be applied instead. The litigant must first identify the applicable rule of foreign law and show that it differs materially from the law in California. If the relevant laws are not materially different, there is no conflict and the court may apply California law. Next, if the laws are materially different, the court must determine each state's interest in having its own law applied. If the interest of the foreign state cannot be established, the court may proceed to apply California law. Finally, if the laws are materially different and each state has an interest in having its own law applied, the court must engage in a "comparative impairment" analysis and determine which state's interest would be more impaired if that state's law were not applied. The court will apply the law of the state whose interest would be more impaired. *Washington Mut. Bank, FA v Superior Court* (2001) 24 C4th 906, 919, 103 CR2d 320. See also *Bernhard v Harrah's Club* (1976) 16 C3d 313, 128 CR 215, cert denied (1976) 429 US 859. A separate "governmental interest" analysis is made for each conflicts issue in the case.

In *Kearney v Salomon Smith Barney, Inc.* (2006) 39 C4th 95, 45 CR3d 730, telephone calls made by California residents to Salomon Smith Barney offices in Georgia were recorded without their consent. The California Supreme Court held that California's stricter privacy laws (which prohibit the recording of phone calls unless all parties consent), rather than Georgia's law (which requires the consent of only one party to the call), would apply to Salomon's future business practices. The court found that California had the greater interest in having its laws applied to the defendant's future conduct, but for past conduct, Georgia law would apply in order not to create an unfair result for Georgia businesses who would otherwise assume that their own state laws governed their activities. 39 Cal. 4th at 102.

© The Regents of the University of California

§19.18 5. Conflicts of Law on Internet

Companies doing business online may find themselves subject to liability based on the laws of other states or even other nations. In a 2002 Internet case, the Australian High Court found that an Australian businessman could bring a libel action in a local Australian court against Dow Jones & Company, an American company, for allegedly defamatory material published in the online version of Barron's (a Dow Jones publication), despite the fact that Dow Jones' website originated from New Jersey. See *Dow Jones & Co. v Gutnick* [2002] HCA 56 (10 Dec 2002), available online at http://www.austlii.edu.au/au/cases/cth/HCA/2002/56.html. The court found that the allegedly defamatory material was "published" in Australia because it was downloadable by paid subscribers there, that the tort was therefore committed in Australia so that Australian law applied, and that Dow Jones had accepted the risk of being sued in Australia by accepting paid subscriptions from Australian residents.

© The Regents of the University of California

B. Choice-of-Law Clauses

1. Enforceability

§19.19 a. California Statutes

Choice-of-law clauses in contracts express the parties' agreement on the law that should govern the validity, interpretation, and performance of their contracts. By statute in California, the parties to any commercial contract involving $250,000 or more that is not for personal services and that does not fall into one of the exceptions in Com C §1105(2) for contracts to which special UCC choice-of-law rules apply (rights of creditors against sold goods, bank deposits and collections, letters of credit, bulk sales, investment securities, secured transactions, and leases) may agree that California law will apply to the contract, even if the contract has no reasonable relationship to the state. Civil Code §1646.5 provides:

> Notwithstanding Section 1646, the parties to any contract, agreement, or undertaking, contingent or otherwise, relating to a transaction involving in the aggregate not less than two hundred fifty thousand dollars ($250,000), including a transaction otherwise covered by subdivision (a) of Section 1301 of the Commercial Code [the basic UCC conflicts-of-law rule, requiring a "reasonable relation" to the state], may agree that the law of this state shall govern their rights and duties in whole or in part, whether or not the contract, agreement, or undertaking or transaction bears a reasonable relation to this state. This section does not apply to any contract, agreement, or undertaking (a) for labor or personal services, (b) relating to any transaction primarily for personal, family, or household purposes, or (c) to the extent provided to the contrary in subdivision (c) of Section 1301 of the Commercial Code.

Choice-of-law clauses in commercial contracts under the UCC involving less than $250,000, which do not fall within the exceptions specified in Com C §1301(c), are subject to the general UCC rule on enforceability in Com C §1301(a):

> [W]hen a transaction bears a *reasonable relation* to this state *and also* to another state or nation, the parties may agree that the law either of this state or of the other state or nation shall govern their rights and duties. [Emphasis added.]

This rule applies to transactions, including e-commerce transactions, in goods under Division 2 of the California Commercial Code. See *Nedlloyd Lines B.V. v Superior Court* (1992) 3 C4th 459, 465 n2, 11 CR2d 330.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/19 Jurisdiction; Conflicts of Law/§19.20 b. Nedlloyd Lines, B.V. v Superior Court and Later Cases

§19.20 b. *Nedlloyd Lines, B.V. v Superior Court* and Later Cases

Choice-of-law clauses that do not fall within CC §1646.5 or Com C §1301(a) (see §19.19) are enforceable in accordance with the standards set forth in *Nedlloyd Lines B.V. v Superior Court* (1992) 3 C4th 459, 11 CR2d 330 (enforcing application of "freely negotiated" choice-of-law provision requiring application of Hong Kong law to contract dispute with Dutch corporation). In *Nedlloyd*, the California Supreme Court expressly adopted the test set out in Restatement (Second) of Conflict of Laws §187(2), holding that (3 C4th at 466, 11 CR2d at 334):

> Briefly restated, the proper approach under Restatement section 187, subdivision (2) is for the court first to determine either: (1) whether the chosen state has a substantial relationship to the parties or their transaction, or (2) whether there is any other reasonable basis for the parties' choice of law. If neither of these tests is met, that is the end of the inquiry, and the court need not enforce the parties' choice of law.… If, however, either test is met, the court must next determine whether the chosen state's law is contrary to a fundamental policy of California.… If there is no such conflict, the court shall enforce the parties' choice of law. If, however, there is a fundamental conflict with California law, the court must then determine whether California has a "materially greater interest than the chosen state in the determination of the particular issue…." (Rest., §187, subd. (2)). If California has a materially greater interest than the chosen state, the choice of law shall not be enforced, for the obvious reason that in such circumstance we will decline to enforce a law contrary to this state's fundamental policy. [Emphasis added.]

See also *Washington Mut. Bank, FA v Superior Court* (2001) 24 C4th 906, 103 CR2d 320 (analyzing enforceability of choice-of-law clause in connection with nationwide certification of class action); *Application Group, Inc. v Hunter Group, Inc.* (1998) 61 CA4th 881, 72 CR2d 73 (invalidating Maryland company's noncompetition agreement with employee later employed by California company as opposed to California's "strong public policy" against such covenants).

NOTE: *Washington Mut. Bank, FA v Superior Court, supra,* is valuable precedent for the enforceability of choice-of-law clauses in online agreements and website terms of use. In that case, the California Supreme Court considered the applicability of the *Nedlloyd* analysis to consumer adhesion contracts. The court noted that there is no public policy in California against enforcement of choice-of-law clauses in adhesion contracts, provided that the clauses otherwise meet the *Nedlloyd* standards. The weaker party to the contract can always seek to avoid the clause on grounds that substantial injustice would result from its enforcement or that the stronger party's use of its bargaining power was unfair. 24 C4th at 918.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/19 Jurisdiction; Conflicts of Law/§19.21 2. Drafting Considerations

§19.21 2. Drafting Considerations

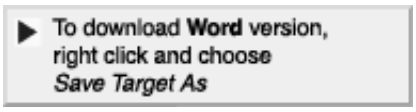
In addition to designating the substantive law of a particular jurisdiction to govern the validity, interpretation, and performance of an agreement, the agreement also should be drafted to exclude the application of conflict-of-law principles (as does the form in §19.22). If the governing law clause excludes the conflicts-of-law rules of a particular jurisdiction, then the court should apply the laws of the agreed jurisdiction to the contract, regardless of where performance of the contract was intended to take place or where the contract was formed. If the conflicts-of-law rules of the designated jurisdiction are not excluded, then the court may look to those conflicts-of-law rules to determine which jurisdiction's substantive law will ultimately govern the contract, and the result may not be consistent with the intent of the parties at the time of contracting. Most choice-of-law clauses are therefore worded to exclude the selected jurisdiction's conflicts-of-law rules.

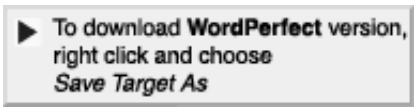
PRACTICE TIP: Choice-of-law clauses are especially important in online contracts because of the global reach of online transactions. Choice-of-law clauses can help an online business avoid costly choice-of-law disputes and unexpected, unfavorable interpretations of their contracts, and help ensure that their contracts will be enforced as intended.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/19 Jurisdiction; Conflicts of Law/§19.22 3. Form: Choice-of-Law Clause

§19.22 3. Form: Choice-of-Law Clause





GOVERNING LAW. This Agreement, and any disputes arising out of this Agreement, shall be interpreted and construed in accordance with the laws of the State of _ _[*name, e.g., California*]**_ _ and the United States, without regard to conflict-of-law principles.**

© The Regents of the University of California

20

Tort and Criminal Liability; First Amendment Issues; Insurance

I. INTRODUCTION §20.1

II. TORT LIABILITY

A. Defamation §20.2

1. Cyberspeech: Libel or Slander? Fact or Opinion? §20.3

2. ISP Liability for Defamation by Subscribers

a. Distributor/Publisher Distinction in Early Cases §20.4

b. Communications Decency Act: Protection for "Good Samaritans" §20.5

c. Scope of Immunity Under CDA §20.6

(1) When Distributor Edits Material §20.6A

(2) How Is Material Collected? §20.6B

(3) When Material Infringes Intellectual Property Rights §20.6C

(4) When Distributor Blocks Objectionable Material §20.6D

d. CDA Preemption of Inconsistent State Law §20.7

B. Rights of Privacy and Publicity

1. Right of Privacy §20.8

2. Right of Publicity §20.9

C. Trespass to Chattels §20.10

D. Conversion §20.11

III. CRIMINAL LIABILITY

A. Generally §20.12

B. Child Pornography §20.13

IV. FREEDOM OF SPEECH

A. Introduction §20.14

B. First Amendment §20.15

C. Obscenity §20.16

D. Child Pornography §20.17

1. Communications Decency Act: Constitutionality Issues §20.18

2. Child Pornography Prevention Act §20.19

3. Child Online Protection Act §20.20

4. Children's Internet Protection Act §20.21

E. California Penal Code §20.22

F. California Education Code §20.22A

G. Filtering Software and the First Amendment §20.23

H. Free Speech Rights in Anonymous Communications; Spam §20.24

I. California Anti-SLAPP Statute §20.25

V. INTERNET COMPLAINT SITES

A. Overview §20.26

B. Potential Causes of Action §20.27

1. Defamation §20.28

2. Trademark Infringement and Dilution §20.29

3. Cybersquatting: Federal and State Law

a. UDRP §20.30

b. Anticybersquatting Consumer Protection Act §20.31

c. California's Anticybersquatting Statute §20.32

C. Practical Solutions §20.33

VI. INSURANCE ISSUES FOR ONLINE BUSINESSES

A. Introduction §20.34

B. Commercial Form General Liability Insurance §20.35

1. Loss of Tangible Property: Is Computer Data "Tangible Property"? §20.36

2. Loss of Tangible Property: Has There Been a "Loss?" §20.37

3. "Physical Loss or Damage" §20.38

4. Intellectual Property Infringement §20.39

C. Business Interruption Coverage §20.40

D. Industry Response §20.41

E. Conclusion §20.42

© The Regents of the University of California

§20.1 I. INTRODUCTION

Previous chapters of this book have addressed many federal and state statutes, as well as some common law theories, that constitute a basis for civil or criminal liability for various types of activities on or relating to the Internet. These include:

- Liability for copyright infringement under the Copyright Revision Act of 1976 (17 USC §§101-1332). See §§1.12-1.17.
- Liability under the anticircumvention provisions of Title I of the Digital Millennium Copyright Act (17 USC §§1201-1205). See §§1.25-1.28.
- Liability for misappropriation of trade secrets under the California Uniform Trade Secrets Act (CC §§3426-3426.11). See §§2.34-2.38.
- Liability for domain name infringement under the Uniform Domain Name Dispute Resolution Policy (UDRP) of the Internet Corporation for Assigned Names and Numbers (ICANN); the federal Anticybersquatting Consumer Protection Act (ACPA) (15 USC §§1125(d), 1129); and the California anticybersquatting statute (Bus & P C §§17525-17528). See §§3.22-3.24.
- Liability for trademark infringement under the Trademark Act of 1946 (also known as the Lanham Act) (15 USC §§1051-1141n), or California state law (Bus & P C §§14200-14272). See §§3.60-3.70.
- Liability under certain federal statutes implicated by copying or transmission of music over the Internet. See §§8.23-8.24.
- Liability under the federal and California state laws protecting rights of privacy. See chap 9.
- Liability for deceptive advertising under the Federal Trade Commission Act (FTC Act) (15 USC §§41-58) or other federal or California state law. See §§17.2-17.10.
- Liability for unsolicited commercial e-mail (spam) under the CAN-SPAM Act of 2003 (Pub L 108-187, 117 Stat 2699), codified primarily at 15 USC §§7701-7713, or California state laws not preempted by the CAN-SPAM Act. See §§17.11-17.29.
- Liability for hacking, dissemination of viruses, use of "web crawlers," or other types of cyberattacks under the Computer Fraud and Abuse Act (CFAA) (18 USC §1030), the Electronic Communications Privacy Act of 1986 (ECPA) (18 USC §§2510-2522, 2701-2712), other federal or California state statutes, and the common law tort of trespass to chattels. See chap 18.

This chapter reviews additional grounds for tort liability for certain online activities, including defamation and the right of publicity, as well as potential criminal liability for child pornography. See §§20.2-20.13. The Communications Decency Act (CDA) (47 USC §230), which offers immunity to Internet service providers from vicarious liability for defamatory statements made by their subscribers, is addressed in §§20.4-20.7. Sections 20.14-20.25 discuss free speech rights under the First Amendment, as well as the California anti-SLAPP statute (CCP §425.16). Obscenity and child pornography in relation to the First Amendment are discussed in §§20.16-20.22. Internet complaint or "gripe" sites are discussed in §§20.26-20.33, including potential causes of action and practical steps that can be taken against "gripe" site operators. Finally, §§20.34-20.42 address insurance issues for online businesses.

Because of the global reach of the Internet, obtaining personal jurisdiction over a defendant is often an issue in Internet-related litigation. Many online businesses lack a physical headquarters in a single jurisdiction and routinely market their products or services across state lines or even internationally. The topic of Internet jurisdiction is discussed in chap 19.

© The Regents of the University of California

II. TORT LIABILITY

§20.2 A. Defamation

Anonymity, data collection possibilities, and global accessibility offered by the Internet have renewed interest in causes of action for defamation and invasion of privacy. Problems unique to the Internet challenge traditional notions of responsibility and liability for acts of defamation, and a body of cyberspace defamation law incorporating state and federal legislative initiatives is emerging.

Elements of the Tort of Defamation. Defamation is (1) a false and unprivileged statement of fact (2) published to someone other than the plaintiff (3) that injures the plaintiff's reputation or tends to injure the plaintiff in his or her occupation. CC §§44-45, 46. See, *e.g.*, *Jensen v Hewlett-Packard Co.* (1993) 14 CA4th 958, 969, 18 CR2d 83. Damages are recoverable for two types of defamation: libel and slander. CC §44.

- Libel is a "writing, printing, picture, effigy, or other fixed representation to the eye" that exposes a person to "hatred, contempt, ridicule, or obloquy, or which causes him to be shunned or avoided, or which has a tendency to injure him in his occupation." CC §45.
- Slander is an oral utterance (including a "communication by radio or any mechanical or other means") that (1) imputes (a) criminality, (b) disease, (c) occupational incompetence or dishonesty, or (d) impotence or want of chastity, or (2) causes actual damage. CC §46.

Publication. Each type of defamation presumes the defendant's publication or utterance of a "false and unprivileged publication." CC §§45-46. A publication must be made to a third person who understands its defamatory meaning. *Dible v Haight Ashbury Free Clinics, Inc.* (2009) 170 CA4th 843, 88 CR3d 464. To be actionable, the publication must be a false statement of fact, rather than a mere statement of opinion. *Gertz v Robert Welch, Inc.* (1974) 418 US 323, 340, 41 L Ed 2d 789, 805, 94 S Ct 2997.

Other Elements. Additional elements are sometimes required for certain defamation actions. For example, if the defamatory statement concerns a for-profit corporation, the plaintiff corporation must also show that the matter tends to prejudice it in the conduct of its business or causes harm to its business reputation. See *DiGiorgio Fruit Corp. v AFL-CIO* (1963) 215 CA2d 560, 571, 30 CR 350; Restatement (Second) of Torts §561 (1977). Public figures who bring defamation actions must also show an element of malice, which requires them to establish that the defendant published the statement knowing it was false or with reckless disregard for the truth. *New York Times Co. v Sullivan* (1964) 376 US 254, 11 L Ed 2d 686, 84 S Ct 710. See also *Ampex Corp. v Cargle* (2005) 128 CA4th 1569, 27 CR3d 863 (website postings about corporation addressed issue of public importance; corporation was limited public figure required to prove malice to prevail).

Publication on the Internet. At common law, a defamatory statement was considered published each time it was distributed. Restatement §577A. The originator of the statement could therefore be held liable each time the statement was repeated if the repetition was reasonably foreseeable. *McKinney v County of Santa Clara* (1980) 110 CA3d 787, 795, 168 CR 89. Under this rule, a plaintiff would have a separate cause of action each time the statement was published—a problematic issue in the context of widespread dissemination of a defamatory statement via mass media. To limit the number of causes of action available to a plaintiff in cases involving mass media, many states, including California, adopted the Uniform Single Publication Act. See CC §§3425.1-3425.5. Under the single-publication rule, publication, a cause of action, and a period of limitation accrue with the first distribution to the public. *Long v Walt Disney Co.* (2004) 116 CA4th 868, 10 CR3d 836. Although the Act does not specify whether it is applicable to publications on the Internet, a court of appeal has held that an Internet website was subject to the single-publication rule notwithstanding that it operated on a continual basis. *Traditional Cat Ass'n v Gilbreath* (2004) 118 CA4th 392, 13 CR3d 353 (posting on Internet website deemed publication as of date it was posted; single-publication rule applies even though statement remains on site and is viewed by others later).

Privileged Statements. A statement that is privileged does not constitute a defamation. Civil Code §47 codifies the privileges that apply to statements that might otherwise be defamatory, such as statements made in the course of legislative or judicial proceedings.

Retractions. Liability in a defamation action may be limited by CC §48a, which provides that a plaintiff who fails to demand a retraction of a defamatory statement made in a newspaper, television, or radio broadcast, or who demands and receives a retraction, is limited in recovery to special damages, defined as damages that the plaintiff "alleges and proves that he has suffered in respect to his property, business, trade, profession or occupation, including such amounts of money" spent as a result of the alleged libel (CC §48a(4)(b)). Although the statutory language does not expressly include Internet publications, it may still be applicable to certain news-oriented websites. See *O'Grady v Superior Court* (2006) 139 CA4th 1423, 1458, 44 CR3d 72 (protection provided by California shield law extends to publication at news website).

© The Regents of the University of California

§20.3 1. Cyberspeech: Libel or Slander? Fact or Opinion?

A defamatory statement published on the Internet, despite its transient nature, is considered libel rather than slander. The California court of appeal addressed the proper cause of action for disparaging statements disseminated on the Internet in *Varian Med. Sys., Inc. v Delfino* (2003) 113 CA4th 273, 6 CR3d 325, rev'd on other grounds (2005) 35 C4th 180, 25 CR3d 298. In an opinion that is now not citable, having been reversed by the California Supreme Court on another issue, the court of appeal held that the defendant's posting of derogatory comments about former supervisors on Internet bulletin boards ("written defamatory communications by means of the Internet") constituted libel. The court reasoned that the defendant's messages were "to the eye" and, unlike the spoken word, were "fixed." See CC §45.

Under defamation law, communications that are clearly expressions of opinion enjoy a qualified privilege and may not be actionable as defamatory if they are not "false statements." See *Gertz v Robert Welch, Inc.* (1974) 418 US 323, 339, 41 L Ed 2d 789, 805, 94 S Ct 2997; *Global Telemedia Int'l, Inc. v Doe 1* (CD Cal 2001) 132 F Supp 2d 1261. See also Restatement (Second) of Torts §566 (1977). Whether a communication is a statement of fact or an opinion is a question of law to be decided by the court. *Baker v Los Angeles Herald Exam'r* (1986) 42 C3d 254, 260, 228 CR 206. Generally, the courts view opinion as "broad, unfocused, and wholly subjective comment." *Fletcher v San Jose Mercury News* (1989) 216 CA3d 172, 191, 264 CR 699.

In determining whether a statement is actionable, the question is not strictly whether it is one of fact or opinion, but rather whether a reasonable factfinder could conclude that it declares or implies a provably false assertion of fact. Opinions stated in e-mail messages were not actionable as libel or trade libel when the messages "fully disclosed provably true facts on which the opinions were based," even though that disclosure was by a direction to the plaintiff's website that contained a "link" to another company's website. *Franklin v Dynamic Details, Inc.* (2004) 116 CA4th 375, 378, 10 CR3d 429 (balancing constitutional guarantees of free speech and prevention of attacks on reputation, court found that reader of otherwise libelous e-mails could view websites and accept or reject e-mailer's opinions). See also *Rocker Mgmt. LLC v John Does 1-20* (ND Cal, May 29, 2003, No. 03-003 3 CRB) 2003 US Dist Lexis 16277, *5 ("free flowing diatribes" posted in Internet chat room that contained warning that messages were "solely the opinion and responsibility of the poster" were not actionable). Although there is a tendency to view Internet bulletin board or chat room postings as expressions of opinion, courts will examine the totality of circumstances in order to determine whether a remark is a statement or implied statement of fact, or merely an opinion. *Global Telemedia Int'l, Inc. v Doe 1* (CD Cal 2001) 132 F Supp 2d 1261, 1267) (statements were not published in manner in which reader would expect to find facts).

Despite a widely held perception that speech over the Internet is anonymous and unregulated, individuals who make libelous statements about others on the Internet may be sued successfully (if they can be found). See, *e.g., Batzel v Smith* (9th Cir 2003) 333 F3d 1018, cert denied (2004) 541 US 1085 ("[t]here is no reason inherent in the technological features of cyberspace why First Amendment and defamation law should apply differently in cyberspace than in the brick and mortar world"). Moreover, recent case law indicates that ISPs and website operators with information about the identity of persons making defamatory statements may be required to divulge their identities, although the process by which those identities must be disclosed is the subject of ongoing litigation. However, in order to protect the First Amendment right to post anonymously on the Internet, a prima facie case for defamation must be shown before a court will issue a subpoena for the disclosure of the identity of an anonymous poster. *Krinsky v Doe 6* (2008) 159 CA4th 1154, 1172, 72 CR3d 231.

For a discussion of the difficulty of locating and identifying online defamation defendants, see *Columbia Ins. Co. v Seescandy.com* (ND Cal 1999) 185 FRD 573, 578 n1. For discussion of the possible use of California's Anti-Strategic Litigation Against Public Participation (Anti-SLAPP) statute (CCP §425.16) as a defensive strategy in defamation actions, see §20.24.

© The Regents of the University of California

2. ISP Liability for Defamation by Subscribers

§20.4 a. Distributor/Publisher Distinction in Early Cases

Early decisions seeking to impose direct or vicarious liability on ISPs for subscriber postings struggled with the application of traditional models of liability to a new medium. The issue, generally, was whether ISPs should be treated like publishers—exercising editorial control over the information they make available and therefore legally accountable for its contents—or like newsstands, bookstores, and other distributors—not necessarily aware of the contents of all the publications they sell and therefore not liable for the contents. Case decisions split along precisely these lines.

In *Cubby, Inc. v CompuServe, Inc.* (SD NY 1991) 776 F Supp 135, a database owner sued CompuServe for libel based on statements about the plaintiff's database in a publication available on CompuServe's "Journalism Forum." The publication containing the allegedly libelous statements was provided by a third party that had no direct relationship, contractual or otherwise, with CompuServe. CompuServe had no opportunity to review the contents of the publication before it was posted to the Journalism Forum. The court held that CompuServe was a distributor, with no editorial control over the publication, and was not subject to liability unless it knew or had reason to know of allegedly defamatory statements.

A few years later, another court reached a different conclusion regarding ISP liability for online defamation. In *Stratton Oakmont v Prodigy Servs., Inc*. (Sup Ct 1995) 1995 NY Misc Lexis 229, a brokerage firm sued Prodigy for allegedly defamatory statements posted on a financial bulletin board operated by Prodigy. The court held that Prodigy was a "publisher" of the allegedly defamatory statements, and therefore subject to liability, regardless of its knowledge of the statement at issue. In distinguishing *Cubby,* the *Stratton Oakmont* court relied on differences in the services provided by Prodigy and CompuServe. Prodigy advertised that, unlike other services, it actively monitored postings to its bulletin boards. Prodigy maintained content guidelines for postings, used software to screen postings for offensive language, and engaged "board leaders" to enforce the content guidelines on certain bulletin boards. The *Stratton Oakmont* holding was quickly superseded by the Communications Decency Act (CDA) (47 USC §230). See §20.5.

© The Regents of the University of California

§20.5 b. Communications Decency Act: Protection for "Good Samaritans"

The so-called "Good Samaritan" provision of the Communications Decency Act (CDA), enacted as Title V of the Telecommunications Act of 1996 (Pub L 104-104, 110 Stat 56), grants limited immunity to internet service providers (ISPs) from defamation liability on account of statements made online by their subscribers. Title 47 USC §230(c)(1) states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." The CDA defines "information content provider" as someone who "is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." 47 USC §230(f)(3). Implicit in the statute is the principle that an ISP *will* be treated as a publisher or speaker to the extent that the ISP itself functions as an "information content provider."

Section 230 does not completely insulate ISPs from liability for defamatory statements provided by others. Many experts believe that liability should still attach when an ISP knows of defamatory material and fails to take any action. See, *e.g., Batzel v Smith* (9th Cir 2003) 333 F3d 1018, cert denied (2004) 541 US 1085 (Gould, J. dissenting) (the "sweeping preemption of valid state libel laws" arguably endorsed by the majority opinion's interpretation of Section 230 "is not necessary to promote Internet use and is not what Congress had in mind.").

NOTE: Parts of the CDA (47 USC §223(a), (d), relating to transmission of obscene material to minors) were held unconstitutional by the Supreme Court in *Reno v ACLU* (1997) 521 US 844, 138 L Ed 2d 874, 117 S Ct 2329. See §20.17. The "Good Samaritan" exemption, however, which was intended to overrule *Stratton Oakmont* (see §20.4) and create incentives for voluntary online content screening, was not affected by the Supreme Court decision.

The "Good Samaritan" exemption under the CDA has two parts: The first, noted above, grants to any "provider or user of an interactive computer service" immunity from liability for republication of any defamatory statement made by another. 47 USC §230(c)(1). *Barrett v Rosenthal* (2006) 40 C4th 33, 57, 51 CR3d 55 (broad immunity of §230(c)(1) applies regardless of whether provider or user viewed as "publisher," "distributor," or "secondary publisher" of allegedly defamatory content). The second part creates broad immunity for ISPs for good faith actions to restrict access to obscene or otherwise objectionable material or to give others the means to do so, even if the material is constitutionally protected (47 USC §230(c)(2)):

No provider or user of an interactive computer service shall be held liable on account of —

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in [subparagraph (A)].

In applying §230, courts have interpreted the term "interactive computer service" (ICS) broadly to "include a wide range of cyberspace services," and not just traditional ISPs. *Batzel*, 333 F3d at 1030. See also *Carafano v Metrosplash.com, Inc.* (9th Cir 2003) 339 F3d 1119 (online matchmaking service held to be ICS); *Corbis Corp. v Amazon.com, Inc.* (WD Wash 2004) 351 F Supp 2d 1090 (defendant providing forums for submission of book reviews considered ICS provider); *PatentWizard, Inc. v Kinko's, Inc.* (D SD 2001) 163 F Supp 2d 1069, 1071 (ISP viewed as ICS); *Gentry v eBay, Inc.* (2002) 99 CA4th 816, 831 n7, 121 CR2d 703 (eBay held to be ICS). A California court decision reviewed the types of entities and services found to be "providers of an interactive computer service," and ruled that the phrase also includes a corporate employer that provides its employees with Internet access through company computers. *Delfino v Agilent Technols., Inc.* (2006) 145 CA4th 790, 806, 52 CR3d 376. Section 230 immunity conferred on an ICS extends to any republication of third party material by individual Internet users. *Barrett v Rosenthal* (2006) 40 C4th 33, 58, 51 CR3d 55.

© The Regents of the University of California

§20.6 c. Scope of Immunity Under CDA

The Communications Decency Act of 1996 (47 USC §230) invalidated previous attempts by the courts to apply traditional defamation analysis to republished cyberspeech. See §20.4. Courts are struggling to define the scope of immunity under §230. In *Zeran v AOL* (4th Cir 1997) 129 F3d 327, cert denied (1998) 524 US 937, the defendant ISP prevailed by asserting §230 as an affirmative defense to liability for defamatory speech initiated by a third party. The court held that §230 foreclosed allegations based on the distinction between distributor and publisher liability.

The California Supreme Court expressed concern about the *Zeran* court's broad grant of immunity in *Barrett v Rosenthal* (2006) 40 C4th 33, 62, 51 CR3d 55:

We share the concerns of those who have expressed reservations about the *Zeran* court's broad interpretation of section 230 immunity. The prospect of blanket immunity for those who intentionally redistribute defamatory statements on the Internet has disturbing implications….[Nevertheless] [p]laintiffs are free under section 230 to pursue the originator of a defamatory Internet publication. Any further expansion of liability must await Congressional action.

Many recent cases have upheld CDA immunity for ISPs, including:

- *Chicago Lawyers' Committee for Civil Rights Under Law, Inc. v Craigslist, Inc.* (7th Cir 2008) 519 F3d 666 (online publisher that did not induce posting of discriminatory housing advertisements protected by §230);
- *Doe v MySpace Inc.* (5th Cir 2008) 528 F3d 413 (MySpace not liable for failure to protect end user who was sexually assaulted by man she met using myspace.com);
- *Universal Communication Sys. v Lycos, Inc.* (1st Cir 2007) 478 F3d 413, 420 (§230 immunity applies even after notice of potentially unlawful nature of third party content);
- *Dart v Craigslist. Inc.* (ND Ill 2009) 665 F Supp 2d 961 (Craigslist immune from liability under §230 for hosting and organizing user-generated classifieds advertising prostitution);
- *Doe v MySpace, Inc.* (ED Tex 2009) 629 F Supp 2d 663 (MySpace protected by §230 where sexual predator used MySpace to communicate with and orchestrate sexual assault on minor);
- *Gibson v Craigslist, Inc.* (SD NY, June 15, 2009, No. 08 Civ 7735) 2009 US Dist Lexis 53246 (Craigslist not liable for shooting of plaintiff with gun purchased on its site);
- *Goddard v Google, Inc.* (ND Cal, Dec. 17, 2008, No. C 08-2738 JF (PVT) 2008 US Dist Lexis 101890 ("Internet content provider" (distinguished by court from "information content provider") not liable for allegedly fraudulent conduct by advertiser); and
- *Doe II v MySpace Inc.* (2009) 175 CA4th 561, 96 CR3d 148 (§230 immunized site from liability when plaintiffs, girls aged 13-15, were sexually assaulted by adults they met through MySpace; characterization of complaint as one for failure to adopt reasonable safety measures did not avoid §230 immunity).

© The Regents of the University of California

§20.6A (1) When Distributor Edits Material

To what degree screening and editing e-mail or other online content can render a distributor an "information content provider" (see §20.5) and thus liable for publishing defamatory material was discussed in *Batzel v Smith* (9th Cir 2003) 333 F3d 1018, cert denied (2004) 541 US 1085. In *Batzel,* a publisher of an online newsletter who selected, minimally edited, and published a potentially defamatory e-mail was held not liable as a content provider. The court cautioned, however, that the service provider could not claim immunity under §230 if it published the defamatory e-mail knowing that it was not intended for publication. 333 F3d at 1034. But see *Best W. Int'l, Inc. v Furber* (D Ariz, Sept. 5, 2008, No. CV-06-1537-PHX-DGC) 2008 US Dist Lexis 70552 (§230 immunity inapplicable to website owner who collaborated in creation of defamatory posts); *John Doe Antiterrorism Officer v City of New York* (SD NY 2008) 583 F Supp 2d 444 (§230 immunity not available when defendant added allegedly tortious speech to forwarded third party content).

In *Carafano v Metrosplash.com, Inc.* (9th Cir 2003) 339 F3d 1119, an online matchmaking service was held to be protected by §230 despite its minor editing of defamatory information submitted by a user who had falsely assumed the identity of an innocent third party. The *Carafano* court noted that even if the defendant could be categorized both as a service provider and, through its use of a questionnaire it formulated, as an information content provider, immunity under §230 would apply unless the defendant "created or developed the particular information at issue." 339 F3d at 1125. In *Carafano,* the court observed that recent decisions have treated the immunity provided by §230 as quite "robust," having adopted a "relatively expansive definition of 'interactive computer service' and a relatively restricting definition of 'information content provider.'" 339 F3d at 1123. But see *Perfect 10, Inc. v CCBill, LLC* (CD Cal 2004) 340 F Supp 2d 1077, 1109 (because "weight of authority supports a finding that the right of publicity is an intellectual property right," California right of publicity claims not subject to §230 immunity).

In *Higher Balance, LLC v Quantum Future Group, Inc.* (D Ore, Dec. 18, 2008, No. 08-233-HA) 2008 US Dist Lexis 102611, an Oregon district court ruled that the defendants could not be held liable for messages posted by website moderators when the plaintiff did not show that the moderators acted under the direction of the site operator. 2008 US Dist Lexis 102611 at *19.

PRACTICE TIP: If a site uses non-employee moderators drawn from the user community in connection with the operation of message boards or other interactive elements of the site, the site operator should prominently clarify that the moderators are unpaid volunteers whose statements and opinions are not controlled or influenced by and do not reflect the opinions of the site operator.

© The Regents of the University of California

§20.6B (2) How Is Material Collected?

The methods used to collect objectionable online content factor into an analysis of whether §230 immunity should be granted. In *Fair Hous. Council v Roommates.com, LLC* (9th Cir 2008) 521 F3d 1157, the Ninth Circuit held that website operators were not immune from liability under §230 because their site forced subscribers to divulge preferences based on protected characteristics for the purpose of matching roommates. Users provided information on roommate preferences using drop-down menus with pre-populated answers indicating, for example, whether the user was willing to live with gay or straight roommates. The court found Roommates.com to be the content provider for the questionnaires and thus responsible for the publication of end-user responses. 521 F3d at 1164. The court sent the following message to website operators seeking immunity under §230: "If you don't encourage illegal content, or design your website to require users to input illegal content, you will be immune." 521 F3d at 1175.

A federal district court in California found a limit on the immunity provided by §230 where a different online matchmaking and dating service was alleged to have created and disseminated false profiles of nonexistent users in order to induce current users to renew their subscriptions to the service. In *Anthony v Yahoo! Inc.* (ND Cal 2006) 421 F Supp 2d 1257, the court rejected an argument by Yahoo! that §230 should bar the plaintiff's fraud and negligent misrepresentation claims. The plaintiff had alleged that Yahoo! originated, created, and perpetuated false and non-existent user profiles so that users would join the service, and then sent fake profiles to users nearing expiration of their subscriptions heralding a "potential new match," so that these users might be persuaded to maintain their memberships. In rejecting the CDA defense, the court held that §230 does not immunize a defendant who—like Yahoo!—is alleged to have created the tortious content, because the statute "only immunizes information provided by *another* information content provider." 421 F Supp 2d at 1263. Because the allegation was that Yahoo! acted as more than simply a publisher or speaker with respect to the false profiles, the §230 defense was not applicable.

In *Goddard v Google, Inc.* (ND Cal 2009) 640 F Supp 2d 1193, the federal district court held that Google had no liability to plaintiffs harmed as a result of clicking on allegedly fraudulent web-based advertisements for mobile subscription services. The court found that harm alleged by the plaintiff resulted from third party content hosted by Google, not from any action by Google, and that §230 protects providers like Google from liability for providing third parties with neutral tools to create web content, even if Google knows the third parties are using them to create illegal content. 640 F Supp 2d at 1198.

© The Regents of the University of California

§20.6C (3) When Material Infringes Intellectual Property Rights

Courts have held that §230 does not protect service providers from claims of direct and contributory intellectual property infringement. In *Gucci Am., Inc. v Hall & Assocs.* (SD NY 2001) 135 F Supp 2d 409, the court held that an ISP that failed to remove trademark infringing material from its website after notice from the trademark holder was not protected by §230, which provides that "[n]othing in the section shall be construed to limit or expand any law pertaining to intellectual property." 47 USC §230(e)(2). See also *Perfect 10, Inc. v. CCBill, LLC* (CD Cal 2004) 340 F Supp 2d 1077, 1108. See also *Doe v Friendfinder Network, Inc.* (D NH 2008) 540 F Supp 2d 288 (right of publicity claim arises out of law of intellectual property and is therefore not barred by §230).

© The Regents of the University of California

§20.6D (4) When Distributor Blocks Objectionable Material

Section 230(c)(2) also contains provisions intended to protect website operators that attempt to block objectionable content. These provisions have been used to shield ISPs from liability for blocking content such as possible e-mail spam. In *e360Insight, LLC v Comcast Corp.* (ND Ill 2008) 546 F Supp 2d 605, the plaintiff claimed its e-mails were being improperly blocked as spam by the defendant's bulk e-mail filtering system. Even if Comcast's filtering software made mistakes, protection under §230 was still appropriate because "Congress, and … everyone else who studied the issue understood that blocking software would probably block too much." 546 F Supp 2d at 607. The court noted that the only way to find Comcast liable would be to find that it did not act in good faith, and the plaintiff had not offered sufficient evidence to support such a finding. 546 F Supp 2d at 609.

In *Zango, Inc. v Kaspersky Lab, Inc.* (9th Cir 2009) 568 F3d 1169, a distributor of Internet security software was held entitled to immunity under §230(c)(2) in a suit claiming that its security software interfered with the use of a third party's downloadable programs. The software helped filter and block Internet-based malicious software from compromising the security or functionality of a user's computer. Because Zango's software incorporated pop-up advertisements and adware, the security software triggered warnings to Zango users and disabled certain features of the Zango software. Holding that §230(c)(2) is intended to "immunize any action taken to enable or make available to others the technical means to restrict access to objectionable material," the court held that the software distributor was entitled to good samaritan immunity. 568 F3d at 1178.

© The Regents of the University of California

§20.7 d. CDA Preemption of Inconsistent State Law

Title 47 USC §230(e)(3) provides in part that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." A California court has permitted a defendant to invoke 47 USC §230 in defense of claims of unfair competition brought under Bus & P C §17200. In *Gentry v eBay, Inc.* (2002) 99 CA4th 816, 121 CR2d 703, the court of appeal declined to hold online auctioneer eBay liable for unfair business practices under Bus & P C §17200 or for violations of CC §1739.7 (a statute governing sports memorabilia dealers) for the sale of sports equipment bearing forged autographs. The court upheld eBay's immunity under 47 USC §230, finding that eBay's compilation of information, even though the information included third-party misrepresentations, did not make eBay an "information content provider." 99 CA4th at 828. See also *Universal Communication Sys. v Lycos, Inc*. (1st Cir 2007) 478 F3d 413 (CDA preempted state securities laws and cyberstalking laws); *Voicenet Communications, Inc. v Corbett* (ED Pa, Aug. 30, 2006, No. 04-1318) 2006 US Dist Lexis 61916 (CDA immunity prevented criminal prosecution of ISP as publisher of third party information); *Doe v America Online* (Fla 2001) 783 So2d 1010 (CDA immunity preempted negligence claims under Florida criminal law). But see *Barrett v Rosenthal* (2006) 40 C4th 33, 64, 51 CR3d 55 (concurring opinion of Moreno, J) (publishers that enter into "tortious conspiracy" to defame with information content provider not protected by §230 immunity).

© The Regents of the University of California

B. Rights of Privacy and Publicity

§20.8 1. Right of Privacy

Federal and California state privacy laws are discussed in chap 9.

© The Regents of the University of California

§20.9 2. Right of Publicity

The common law right of publicity is one aspect of the right of privacy. It is the exclusive right that every person has to control the commercial exploitation of his or her image. See generally *Zacchini v Scripps-Howard Broadcasting Co*. (1977) 433 US 562, 570, 53 L Ed 2d 965, 97 S Ct 2849. California recognizes two causes of action based on the right of publicity. First is the common law right, the elements of which are (*Gionfriddo v Major League Baseball* (2001) 94 CA4th 400, 409, 114 CR2d 307):

- The defendant's use of the plaintiff's identity;
- The appropriation of plaintiff's name or likeness to defendant's advantage, commercially or otherwise;
- Lack of consent; and
- Resulting injury.

The common law right also requires that the right of publicity "be balanced against the public interest in the dissemination of news and information consistent with the democratic processes under the constitutional guaranties of freedom of speech and of the press." 94 CA4th at 409. See also *Perfect 10, Inc. v Cybernet Ventures, Inc.* (CD Cal 2002) 213 F Supp 2d 1146, 1183. In addition, the right of publicity is statutory in California. Under CC §3344,

[a]ny person who knowingly uses another's name, voice, signature, photograph, or likeness, in any manner, on or in products, merchandise, or goods, or for purposes of advertising or selling, or soliciting purchases of, products, merchandise, goods or services, without such person's prior consent, or, in the case of a minor, the prior consent of his parent or legal guardian, shall be liable for any damages sustained by the person or persons injured as a result thereof.

The statutory remedy provided in CC §3344 requires the plaintiff to allege two additional elements: "knowing use" of plaintiff's likeness and a direct connection between the use and a commercial purpose. *Downing v Abercrombie & Fitch* (9th Cir 2001) 265 F3d 994, 1001.

In *Laws v Sony Music Entertainment, Inc.* (9th Cir 2006) 448 F3d 1134, the Ninth Circuit held that federal copyright law could preempt a right of publicity claim arising under state law. The court adopted a two-part test to determine whether a state law could be preempted by the federal Copyright Act:

- The state law claim must fall within the subject matter of copyright.
- The rights protected under state law must be equivalent to the rights of the copyright holders.

448 F3d at 1138.

Defendants in actions for commercial misappropriation may assert First Amendment defenses related to freedom of expression and public interest. See *Daly v Viacom, Inc.* (ND Cal 2002) 238 F Supp 2d 1118 (although defendants used excerpt containing plaintiff's image to advertise their television program and were unable to persuade court that their program was of public interest, their use of excerpt qualified for First Amendment protection as "exposition of ideas").

© The Regents of the University of California

§20.10 C. Trespass to Chattels

Application of the common law tort of trespass to chattels to hacking and other cyberattacks is discussed in §§18.17-18.21.

© The Regents of the University of California

§20.11 D. Conversion

California recognizes that the common law tort of conversion applies to intangible property, even in circumstances where the intangible property right is not represented by or merged with a physical document. See *Kremen v Cohen* (9th Cir 2003) 337 F3d 1024, 1029; *Payne v Elliot* (1880) 54 C 339; *A&M Records, Inc. v Heilman* (1977) 75 CA3d 554, 142 CR 390, cert denied (1977) 436 US 952. In this respect, California law differs from the rule stated in the Restatement (Second) of Torts §242 (1977). In *Kremen v Cohen, supra,* a domain name registrar transferred a domain name to a con man based on a forged letter. The Ninth Circuit Court of Appeals held that the right to use a domain name is an intangible personal property right protected by California conversion law. See also *Bancroft & Masters, Inc. v Augusta Nat'l, Inc*. (9th Cir 2000) 223 F3d 1082, 1089. However, state law claims of conversion may be preempted by copyright claims. In *Healthcare Advocates, Inc. v Harding, Earley, Follmer & Frailey* (ED Pa 2007) 497 F Supp 2d 627, the court concluded that the elements for common law conversion and trespass to chattel were the same as the elements for copyright infringement. Consequently, the claim under the Copyright Act preempted the state common law claims. 497 F Supp 2d at 650.

© The Regents of the University of California

III. CRIMINAL LIABILITY

§20.12 A. Generally

Online businesses are generally subject to the same criminal laws that govern "brick and mortar" businesses and in addition may be subject to criminal liability under a number of federal or state statutes more particularly addressed to computer or Internet-related crimes, as listed in §20.1. These statutes typically provide both civil and criminal penalties, depending on the severity of the offense and whether the requisite criminal intent is present.

NOTE: Penal Code §653.2 makes the use of a computer or other electronic communication device to injure or harass another person a misdemeanor.

In *Mazur v eBay Inc.* (ND Cal, July 25, 2008, No. C 07-03967 MHP) 2008 US Dist Lexis 57105, the federal district court denied defendant eBay's motion to dismiss a RICO (Racketeer Influenced and Corrupt Organizations Act) (18 USC §§1961-1968) claim based on allegations of shill bidding in third party live auctions. Although eBay had provided access to the auctions via its website since July 2004, eBay consistently asserted that each auction was "safe" and "carefully screened." The court found eBay's conduct exhibited the "pattern of racketeering activity" sufficient to allow plaintiff's claim under 18 USC §1962(c) to survive eBay's motion to dismiss.

© The Regents of the University of California

§20.13 B. Child Pornography

Federal law makes it illegal to distribute or possess child pornography. 18 USC §2251. In general, pornography can be banned only if obscene under constitutional standards (see §20.16), but pornography showing minors can be prohibited whether or not the images are obscene. *Ashcroft v Free Speech Coalition* (2002) 535 US 234, 240, 152 L Ed 2d 403, 418, 122 S Ct 1389. Both federal and state lawmakers have been active in attempting to control online child pornography. For example, under the Providing Resources, Officers, and Technology to Eradicate Cyber Threats to Our Children Act of 2008 (PROTECT Our Children Act of 2008) (Pub L 110-401, 122 Stat 4229, codified primarily at 18 USC §§2258A-2258D and 42 USC §§17611-17617), any time an ISP learns that its services are being used to transmit child pornography, the ISP is required to report the facts and circumstances to the Cyber Tipline at the National Center for Missing and Exploited Children, http://www.missingkids.com. 18 USC §2258A(a). Reports may include information about child pornography images, identities of persons sending or receiving child pornography, and requests by individuals to receive child pornography. 18 USC §2258A(b); 18 USC §2702(b)(6). The Act imposes fines for knowingly and willfully failing to report. 18 USC §2258A(b)(e). As an incentive for ISPs to report, the Act bars civil suits against ISPs for any action taken in good faith to comply with its requirements. 18 USC §2258B.

The knowing transport, receipt, distribution, sale, or possession in interstate commerce, by any means including by computer, of any visual depictions of minors engaged in sexually explicit acts is a federal crime. See 18 USC §2252(a); *U.S. v Hockings* (9th Cir 1997) 129 F3d 1069 (computer GIF files were "visual depictions"). Further, it is illegal to receive, copy, or distribute any image simulating child pornography. 18 USC §2252A. The statute provides an affirmative defense if the defendant can show that the actor was an adult at the time the image was created and that it was not distributed or promoted as child pornography. 18 USC §2252A(c). In addition, state statutes controlling child pornography may implicate ISPs, online chat rooms, and similar online services whose users are engaged in criminal behavior. See generally Pen C §§311-311.11 (regulation of "obscene" materials includes computer software, CD-ROMs, and various other kinds of computer-generated and computer-readable materials).

Other federal and state laws that seek to restrict online child pornography, including Child Pornography Prevention Act of 1996 (CPPA) (18 USC §§2251-2260), are discussed in §§20.17-20.22. Title 18 USC §1465, discussed in §20.16, generally criminalizes any distribution in interstate commerce, by any means, including an interactive computer service, of obscene material or other material of indecent or immoral character. This statute is not limited to minors.

© The Regents of the University of California

IV. FREEDOM OF SPEECH

§20.14 A. Introduction

Sections 20.15-20.25 provide an overview of free speech principles and the free speech issues in cyberspace that are most likely to affect companies with online operations. In general, the First Amendment is somewhat a double-edged sword for online businesses. Some aspects of the law of free speech protect businesses operating online, while other aspects restrict, or create liability for, online activities. Companies doing business on the Internet are often required to balance competing interests under the First Amendment.

Sections 20.16-20.22 discuss First Amendment issues relating to obscenity and pornography. The use of content filters, including filters for adult content and First Amendment limitations on their use, are discussed in §20.23. Section 20.24 addresses the scope of First Amendment protection for anonymous and pseudonymous speech on the Internet. California's anti-SLAPP statute is discussed in §20.25.

© The Regents of the University of California

§20.15 B. First Amendment

The First Amendment to the United States Constitution mandates that "Congress shall make no law… abridging the freedom of speech…." By operation of the Fourteenth Amendment, the First Amendment also binds state and local governments, as well as governmental agencies and institutions such as public school systems, state colleges and universities, and public libraries. In general, the scope of free speech protection under the First Amendment extends to speech in cyberspace. For example, as discussed in §20.21, the First Amendment is implicated when public libraries install blocking or filtering software on library computer terminals to prevent access by minors to pornographic material.

As a general rule, the First Amendment prevents the government from dictating what the public should see, read, speak, or hear. The scope of First Amendment protection of speech is limited, however. It does not embrace certain categories of speech, including defamation, incitement, obscenity, and pornography produced with real children. *Ashcroft v Free Speech Coalition* (2002) 535 US 234, 245, 152 L Ed 2d 403, 418, 122 S Ct 1389. As Justice Holmes famously wrote, "The most stringent protection of free speech would not protect a man in falsely shouting fire in a theatre and causing a panic." *Schenk v U.S.* (1919) 249 US 47, 52, 63 L Ed 470, 473, 39 S Ct 247. The First Amendment does not create an absolute privilege for expressions of opinion against liability under state defamation laws. *Milkovich v Lorain Journal Co.* (1990) 497 US 1, 111 L Ed 2d 1, 110 S Ct 2695. Similarly, First Amendment protection does not extend to "those personally abusive epithets which, when addressed to the ordinary citizen, are, as a matter of common knowledge, inherently likely to provoke violent action." *Cohen v California* (1971) 403 US 15, 20, 29 L Ed 2d 284, 291, 91 S Ct 1780. This definition of the "fighting-words doctrine" is generally understood to permit government regulation of speech only in those instances when the speech is addressed directly (*i.e.,* face to face) to another person and the utterance is likely to provoke an "immediate violent response" in the addressee. See *Gooding, Warden v Wilson* (1972) 405 US 518, 528, 31 L Ed 2d 408, 417, 92 S Ct 1103. Because online communications and correspondence—even real-time interactions like chat and instant messaging—lack the face-to-face component required by the "fighting words" doctrine, it seems unlikely that the doctrine applies in cyberspace. However, First Amendment protection does not extend to true "threats of force." *Planned Parenthood v American Coalition of Life Activists* (9th Cir 2002) 290 F3d 1058 (list of names and addresses of abortion providers posted on website constituted true "threat of force" to providers; it was therefore unprotected speech).

The U.S. Supreme Court has long recognized that obscene or pornographic material does not enjoy unlimited First Amendment protection, and may be restricted or prohibited—both online and off—according to standards articulated in U.S. Supreme Court decisions. See §§20.16-20.22.

© The Regents of the University of California

§20.16 C. Obscenity

Affirming its prior holding in *Roth v U.S.* (1957) 354 US 476, 1 L Ed 2d 1498, 77 S Ct 1304, the Supreme Court in *Miller v California* (1973) 413 US 15, 36, 37 L Ed 2d 419, 438, 93 S Ct 2607, confirmed that obscene material is not protected by the First Amendment. At the same time, because of "the inherent dangers of undertaking to regulate any form of expression," the Court required that state criminal statutes "designed to regulate obscene materials must be carefully limited." 413 US at 23, 37 L Ed 2d at 430. Enunciating a three-part test for determining whether a work may be regulated as obscene, the court held that obscenity exists where (413 US at 24, 37 L Ed 2d at 431):

(1) the average person, applying contemporary community standards, would find that the work, taken as a whole, appeals to the prurient interest; (2) the materials depict or describe in a patently offensive way, sexual conduct specifically prohibited by applicable state law; and (3) the work, taken as a whole, lacks serious literary, artistic, political or scientific value.

The *Miller* test's reliance on community standards is problematic in an Internet context, because materials available online probably cannot be kept out of jurisdictions where local community standards might deem them obscene. See 413 US at 30, 37 L Ed 2d at 434. One widely reported case, *U.S. v Thomas* (6th Cir 1996) 74 F3d 701, illustrates the jurisdictional problems faced by online businesses. In *Thomas,* husband and wife operators of an electronic bulletin board system (BBS) based in Milpitas, California, were convicted in Tennessee under federal obscenity laws for providing subscribers with access to sexually explicit images. The defendants were indicted on 12 counts, including six counts under 18 USC §1465 for "knowingly using and causing to be used a facility and means of interstate commerce—a combined computer/telephone system—for the purpose of transporting obscene, computer-generated materials (the [scanned computer] files) in interstate commerce." 74 F3d at 706. The court rejected the defendants' argument that they should have been tried in California, not Tennessee, holding that "the effects of the Defendants' criminal conduct reached the Western District of Tennessee," and that defendants were therefore subject to prosecution in Tennessee. 74 F3d at 710.

Federal law generally prohibits the transportation of obscene material in interstate commerce for purposes of sale or distribution and also bars the importation of obscene materials. See 18 USC §§1460-1466. The code includes a specific reference to transportation by "an interactive computer service" (18 USC §1465):

Whoever knowingly produces with the intent to transport, distribute, or transmit in interstate of foreign commerce, or whoever knowingly transports or travels in, or uses a facility or means of, interstate or foreign commerce or an interactive computer service (as defined in section 230(e)(2) of the Communications Act of 1934 [47 USC §230(e)(2)]) in or affecting such commerce, for the purpose of sale or distribution of any obscene, lewd, lascivious, or filthy book, pamphlet, picture, film, paper, letter, writing, print, silhouette, drawing, figure, image, cast, phonograph recording, electrical transcription or other article capable of producing sound or any other matter of indecent or immoral character, shall be fined under this title or imprisoned not more than five years, or both.

Liability for transportation of obscene material is not necessarily limited to senders and recipients. In *U.S. v Thomas* (6th Cir 1996) 74 F3d 701, the court held that operation of a BBS that allowed subscribers to download and order obscene material violated federal obscenity laws.

A listing of federal criminal laws regulating obscenity and their prescribed punishments can be found at http://www.usdoj.gov/criminal/ceos/obscenity_stats.html. Using misleading domain names to deceive a person into viewing obscene material is included among the crimes codified, with possible imprisonment for up to two years. 18 USC §2252B(a).

© The Regents of the University of California

§20.17 D. Child Pornography

Many U.S. Supreme Court decisions, including *Ginsberg v New York* (1968) 390 US 629, 20 L Ed 2d 195, 88 S Ct 1274, and *New York v Ferber* (1982) 458 US 747, 73 L Ed 2d 1113, 102 S Ct 3348, have recognized the government's interest in protecting children and have upheld obscenity laws that apply different standards to protect minors than might apply to adults. Beginning in the mid-1990s, a number of federal legislative initiatives sought to prevent both online access by children to adult pornographic materials and the general availability of child pornography online. See §§20.13, 20.18-20.21. In some cases, these laws did not survive First Amendment challenges because they were not sufficiently narrow in scope, *i.e.,* they would have restricted access to constitutionally protected material as well as obscene materials. See, *e.g., Ashcroft v Free Speech Coalition* (2002) 535 US 234, 152 L Ed 2d 403, 122 S Ct 1389. Sections 20.18-20.22 discuss certain federal laws regulating child pornography that Internet service providers (ISPs), online chat services, and other online businesses should be aware of, including some that have run afoul of the First Amendment.

© The Regents of the University of California

§20.18 1. Communications Decency Act: Constitutionality Issues

In addition to the "Good Samaritan" provisions intended to protect ISPs, discussed in §20.5, the Communications Decency Act (CDA) (*47* USC §223) was intended to regulate a wide range of allegedly indecent online activity, including the dissemination via the Internet of obscene material to children. In its original form, *47* USC §223 prohibited the transmission of "lewd, lascivious, filthy, or indecent" messages to any recipient under the age of 18, as well as the sending or displaying of material through an interactive computer service that "in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs" to a person under the age of 18. These two provisions came to be known as the "indecent transmission" provision and the "patently offensive display" provision. See *Reno v ACLU* (1997) 521 US 844, 858, 138 L Ed 2d 874, 889, 117 S Ct 2329.

In *Reno v ACLU,* the Supreme Court ruled that the "indecent transmission" and "patently offensive display" provisions of the CDA were overbroad and unconstitutional. The Court found that the CDA criminalized protected speech (including sexually explicit speech) as well as unprotected obscenity and that its vague language chilled free speech, because speakers could not ascertain whether their speech was prohibited. The Court criticized the CDA as not having been "carefully tailored to the congressional goal of protecting minors from potentially harmful materials." 521 US at 871, 138 L Ed 2d at 897. The Court held (521 US at 874, 138 L Ed 2d at 899):

In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another. That burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve.

The Court left intact §223(a) by severing the indecency provision and limiting its application to obscene communications. 521 US at 882, 138 L Ed 2d at 904. Currently, the CDA prohibits the communication of obscene material and child pornography in interstate commerce. Violators are subject to fines and imprisonment of up to 2 years. *47* USC §223(a).

As noted in §20.5, the "Good Samaritan" provision of the CDA was not invalidated by the Supreme Court's decision in *Reno v ACLU*.

© The Regents of the University of California

§20.19 2. Child Pornography Prevention Act

The Child Pornography Prevention Act of 1996 (CPPA) (18 USC §§2251-2260) prohibits sexual exploitation of children and child pornography. Under the CPPA, it is a felony to employ or persuade a minor to engage in sexually explicit conduct for the purpose of producing a visual depiction of such conduct. 18 USC §2251(a). In addition, CPPA prohibits transporting, shipping, receiving, or distributing in interstate or foreign commerce, including by computer, any visual depiction "if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and such visual depiction is of such conduct." 18 USC §2252(a). The legal definition of "sexually explicit conduct" is not limited to depictions of sexual activity; it extends to images of naked minors if such images are sexually suggestive. See 18 USC §2256(2); http://www.usdoj.gov/criminal/ceos/citizensguide_porn.html. Federal law considers any person under the age of 18 to be a minor (18 USC §2256(1)), irrespective of state laws. Violations are punishable by a fine, imprisonment of up to 15 years, or both. 18 USC §2252(b).

CPPA contains affirmative defenses that may be asserted if the material alleged to be child pornography was in fact created using adults and "defendant did not advertise, promote, present, describe, or distribute the material in such a manner as to convey the impression that it is or contains a visual depiction of a minor engaging in sexually explicit conduct." 18 USC §2252A(c)-(d). Another affirmative defense is possessing less than three images of child pornography and promptly, in good faith, taking reasonable steps to destroy the images or reporting the material to a law enforcement agency and giving the agency access to the images. 18 USC §2252A(d).

In *Ashcroft v Free Speech Coalition* (2002) 535 US 234, 152 L Ed 2d 403, 122 S Ct 1389, the Supreme Court struck down two subsections of the CPPA, 18 USC §2256(8)(B) and (D), that criminalized "virtual" child pornography by prohibiting any visual depiction that "is, or *appears to be,* of a minor engaging in sexually explicit conduct" (emphasis added). The Court faulted the CPPA provisions as overbroad, for prohibiting speech that was neither obscene nor child pornography and therefore abridging a substantial amount of constitutionally protected speech. "[S]peech within the rights of adults to hear may not be silenced completely in an attempt to shield children from it.… [T]he State [can]not 'reduce the adult population … to reading only what is fit for children' (citations omitted)." 535 US at 251, 152 L Ed 2d at 422.

In 2003, in response to the *Ashcroft v Free Speech Coalition* decision, Congress amended the CPPA by substituting language in 18 USC §2256(8)(B) to include in the definition of "child pornography" any visual depiction that "is a digital image, computer image, or computer-generated image that is, or *is indistinguishable from,* that of a minor engaging in sexually explicit conduct" (emphasis added), and by deleting 18 USC §2256(8)(D) altogether. The prescribed punishments for CPPA violations are:

- Production of child pornography: Not less than 15 years, not more than 30 years (18 USC §2251).
- Selling or buying children for sexual exploitation: Not less than 30 years or for life (18 USC §2251A).
- Possession, distribution, or receipt of child pornography: Mandatory minimum of 5 years for distribution or receipt, not more than 20 years (18 USC §§2252-2252A).
- Importation of child pornography (enticing a minor): Not less than 15 years, not more than 30 years (18 USC §2260(a), (c)).
- Importation of child pornography (depiction of minor): Not less than 5 years, not more than 20 years (18 USC §2260(b), (c)).

© The Regents of the University of California

§20.20 3. Child Online Protection Act

The Child Online Protection Act of 1998 (COPA) (47 USC §231) prohibited anyone from (47 USC §231(a)(1)):

knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, mak[ing] any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors.

COPA relied on "contemporary community standards" to define material that is harmful to minors. See 47 USC §231(e)(6). In the context of the Internet, the community is a national one; it follows that a standard for as large and varied a community may of necessity be overly broad. COPA was challenged before taking effect on the grounds that it was unconstitutionally vague and overbroad; the U.S. District Court for the Eastern District of Pennsylvania enjoined enforcement of the statute. The case eventually reached the Supreme Court, which upheld the injunction, finding that the government failed to rebut plaintiffs' claim that there were "plausible, less restrictive alternatives to the statute." *Ashcroft v ACLU* (2004) 542 US 656, 666, 159 L Ed 2d 690, 702, 124 S Ct 2783. In March 2007, COPA was declared unconstitutional as overbroad, vague, and not sufficiently narrowly tailored to meet its goals. See *ACLU v Gonzales* (ED Pa 2007) 478 F Supp 2d 775, aff'd sub nom *ACLU v Mukasey* (3d Cir 2008) 534 F3d 181, cert denied (2009) ___ US ___, 173 L Ed 2d 293, 129 S Ct 1032.

NOTE: It is important to distinguish COPA from the Children's Online Privacy Protection Act of 1998 (COPPA) (15 USC §§6501-6506), discussed in §§9.26-9.31, which is an entirely different federal law protecting children from online exploitation.

© The Regents of the University of California

§20.21 4. Children's Internet Protection Act

The Children's Internet Protection Act (CIPA), Pub L 106-554, 113 Stat 2763, codified at 20 USC §9134 and 47 USC §254, requires Internet content filtering by public schools and libraries receiving federal grant funds for Internet access terminals in order to protect minors from receiving obscene or pornographic material. A group of plaintiffs that included the American Library Association challenged the constitutionality of CIPA. A three-judge district court panel held the law unconstitutional because the available filtering technology would result in blocking substantial amounts of protected speech. *American Library Ass'n v U.S.* (ED Pa 2002) 201 F Supp 2d 401, rev'd (2003) 539 US 194. The Supreme Court, however, reversed the district court and declared CIPA constitutional, holding that CIPA was a valid exercise of Congress's spending power, and was consistent with the traditional role of libraries to facilitate research, learning, and recreational pursuits by selecting materials for their collections of appropriate quality. Libraries were not "public forums" and could lawfully exclude obscene materials from their print collections. Adults wishing to access restricted materials could request that blocking software be disabled or removed for the period of their use. *U.S. v American Library Ass'n* (2003) 539 US 194, 156 L Ed 2d 221, 123 S Ct 2297. California has a law requiring state-funded libraries that provide Internet access to their patrons to adopt a policy regarding Internet access by minors. Ed C §18030.5.

To the extent that libraries do not receive state or federal funding, they are not required to comply with the foregoing laws on filtering or Internet access by minors. For a discussion of laws on child pornography, Internet access by minors, and the role and obligations of libraries in applying these laws, see American Library Association, *CPPA, COPA, CIPA: Which Is Which?*, available at http://www.ala.org/ala/aboutala/offices/oif/ifissues/issuesrelatedlinks/cppacopacipa.cfm.

© The Regents of the University of California

§20.22 E. California Penal Code

Penal Code §§313-313.5 prohibit persons who know they are dealing with a minor, or those who fail to exercise reasonable care in ascertaining the true age of a minor, from selling, distributing, sending, offering, or distributing any harmful matter by any means to a minor. Pen C §313.1. "Harmful matter" is defined as (Pen C §313(a))

matter, taken as a whole, which to the average person, applying contemporary statewide standards, appeals to the prurient interest, and is matter which, taken as a whole, depicts or describes in a patently offensive way sexual conduct and which, taken as a whole lacks serious literary, artistic, political or scientific value for minors.

Violations of §313.1 are punishable by a fine, imprisonment, or both. Pen C §313.4.

In 2008, the legislature amended the Penal Code to address harassment by electronic means, targeting anyone who (Pen C §653.2(a))

electronically distributes, publishes, e-mails, hyperlinks, or makes available for downloading, personal identifying information, including, but not limited to, a digital image of another person, or an electronic message of a harassing nature about another person.

"Harassment" is defined as "a knowing and willful course of conduct … that a reasonable person would consider as seriously alarming, seriously annoying, seriously tormenting, or seriously terrorizing the person and that serves no legitimate purpose." Pen C §653.2(c)(1).

© The Regents of the University of California

§20.22A F. California Education Code

The California Legislature has also amended the Education Code to control bullying "committed … by means of an electronic act" in schools. Ed C §§32261(d), 32265(b)(9), 48900(r). An electronic act includes "a message, text, sound, or image by means of an electronic device, including, but not limited to, a telephone, wireless telephone or other wireless communication device, computer, or pager." Ed C §32261(g). Bullying by means of an electronic act is one of the grounds for suspension or expulsion from school. Ed C §48900(r).

© The Regents of the University of California

§20.23 G. Filtering Software and the First Amendment

Filtering software offers a means for restricting online access to obscene or pornographic material. Typical filtering software programs search for objectionable key words and block access to websites that contain those words. Filters are problematic and have been criticized for a number of reasons. First, filters generally search only for text and not images, limiting their utility in a medium as graphic-intensive as the World Wide Web. In addition, filters tend to err on the side of overbreadth: Websites are identified by the presence of certain key words, not reviewed for content. As a result, filters may be unable to distinguish between adult-themed websites, on the one hand, and websites about "breast cancer" or even "chicken breasts" on the other. As recently as July 2003, studies of leading "blocking software" programs found substantial overblocking of content that was permissible to view, as well as substantial underblocking of prohibited content. See Sinrod, *CIPA-Regulated Filters Fall Far Short*, USAToday.com, July 24, 2003, available at http://www.usatoday.com/tech/columnist/ericjsinrod/2003-07-22-sinrod_x.htm.

Filtering can be implemented through server-side or client-side software. An ISP performs server-side filtering, by which the ISP's server denies all subscribers access to content selected for blocking. Client-side filtering operates on end users' computers by restricting a web browser from downloading content from certain specified content sources. Parental controls usually take the form of client-side filtering, and allow parents to disable the filters when they wish to use the computer.

The use of filters by government agencies may implicate First Amendment concerns to the extent that the filters restrict speech that is protected under the First Amendment. See §20.20. Filtering by public schools and libraries, however, has been sanctioned (see *U.S. v American Library Ass'n* (2003) 539 US 194, 156 L Ed 2d 221, 123 S Ct 2297), as has the right of states to screen and block content on state computers. See *Urofsky v Gilmore* (4th Cir 2000) 216 F3d 401, cert denied (2001) 531 US 1070 (state restriction on employees' access to Internet materials did not affect private free speech rights and therefore did not implicate First Amendment).

© The Regents of the University of California

§20.24 H. Free Speech Rights in Anonymous Communications; Spam

"[A]n author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment." *McIntyre v Ohio Elections Comm'n* (1995) 514 US 334, 342, 131 L Ed 2d 426, 436, 115 S Ct 1511. This principle applies particularly to anonymous political speech, such as handbills and leaflets expressing political views, as well as to literary publications. *McIntyre v Ohio Elections Comm'n*, *supra*; *Talley v California* (1960) 362 US 60, 4 L Ed 2d 559, 80 S Ct 536. Courts have held that civil subpoenas seeking to identify anonymous individuals raise First Amendment concerns. *Sony Music Entertainment v Does* (SD NY 2004) 326 F Supp 2d 556, 563. Generally, First Amendment protection has been afforded to anonymous speakers to protect against the use of "discovery procedures to ascertain the identities of unknown defendants in order to harass, intimidate, or silence critics in the public forum opportunities presented by the Internet." *Dendrite Int'l, Inc. v Doe 3* (NJ Super 2001) 775 A2d 756, 771. The right to speak anonymously, however, does not shield the speaker from all potential liability for defamation.

In *Dendrite*, the plaintiff corporation sought discovery of the identity of an anonymous poster on a Yahoo! message board who had posted allegedly defamatory statements concerning the plaintiff's stock. The court affirmed the trial court's denial of discovery on grounds that the plaintiff had failed to establish that the defendant's statements constituted actionable defamation. The New Jersey court stated that, in considering such discovery requests, the trial court must balance "the First Amendment right to speak anonymously, and the right of the plaintiff to protect its proprietary interests and reputation through the assertion of recognizable claims based on the actionable conduct of the anonymous, fictitiously-named defendants." 775 A2d at 760. See also *Best W. Int'l, Inc. v Doe* (D Ariz, July 25, 2006, No. CV061537) 2006 US Dist Lexis 56014 (summary judgment standard must be met before plaintiff can discover identities of Doe defendants); *Doe v Cahill* (Del Super 2005) 884 A2d 451 (reversing lower court that had rejected *Dendrite* and instead had applied lesser "good faith" standard to plaintiffs' effort to discover identity of anonymous Internet posters).

In *Columbia Ins. Co. v Seescandy.com* (ND Cal 1999) 185 FRD 573, the court set forth a four-part test for uncovering the identity of an anonymous individual. The plaintiff must (185 FRD at 578):

- Identify the missing party sufficiently enough to determine whether the party is real and capable of being sued in federal court;
- Reveal all steps taken to locate the missing party;
- Establish that plaintiff's claim could withstand a motion to dismiss; and
- File a discovery request with a statement of reasons justifying the specific discovery requested and identify a limited number of persons or entities to be served "for which there is a reasonable likelihood that the discovery process will lead to identifying information about defendant that would make service of process possible."

The applicability of the First Amendment to unsolicited commercial e-mail ("spam") was at issue in *Cyber Promotions, Inc. v America Online, Inc.* (ED Pa 1996) 948 F Supp 436. Plaintiff Cyber Promotions, Inc. sued AOL after AOL blocked the plaintiff's efforts to send unsolicited e-mail advertisements over the Internet to AOL subscribers. The federal district court ruled that the plaintiff did not have a First Amendment right to send spam, and that AOL, as a private company, had the right to block it in any event. The First Amendment protects against actions by federal, state, or local governments; it does not protect against the conduct of private persons or businesses such as AOL. But see *Jaynes v Commonwealth* (Va 2008) 666 SE2d 303 (prohibition of all unsolicited bulk e-mail, including e-mail containing political, religious, or other protected speech, was overbroad and unconstitutional). See chap 17 for further discussion of spam and recent anti-spam legislation.

© The Regents of the University of California

§20.25 I. California Anti-SLAPP Statute

California's Anti-Strategic Litigation Against Public Participation (Anti-SLAPP) statute (CCP §425.16) was adopted specifically to reduce the incidence of lawsuits brought to chill the valid exercise of the constitutional right of freedom of speech and the right to petition for redress of grievances. The statute provides that a defendant in "a cause of action against a person arising from any act of that person in furtherance of the person's right of petition or free speech under the United States or California Constitution in connection with a public issue" may file a special motion to strike the plaintiff's complaint. CCP §425.16(b)(1). A motion to strike should be filed within 60 days of service of the complaint. CCP §425.16(f). The phrase "act in furtherance of a person's right of petition or free speech under the United States or California Constitution in connection with a public issue" is defined to include (CCP §425.16(e)):

(1) any written or oral statement or writing made before a legislative, executive, or judicial proceeding, or any other official proceeding authorized by law; (2) any written or oral statement or writing made in connection with an issue under consideration or review by a legislative, executive, or judicial body, or any other official proceeding authorized by law; (3) any written or oral statement or writing made in a place open to the public or a public forum in connection with an issue of public interest; (4) or any other conduct in furtherance of the exercise of the constitutional right of petition or the constitutional right of free speech in connection with a public issue or an issue of public interest.

A public website does not have to allow open forums or other forms of public participation to be considered a public forum. See *Wilbanks v Wolk* (2004) 121 CA4th 883, 897, 17 CR3d 497. In order for the plaintiff's lawsuit to survive the motion to strike, the plaintiff must establish a probability that it will prevail on the merits. *Batzel v Smith* (9th Cir 2003) 333 F3d 1018, 1024, cert denied (2004) 541 US 1085. A prevailing defendant is entitled to recover attorney fees and costs. The statute exempts certain actions brought by state and local attorneys. See §425.16(d).

Defendants in libel actions have successfully applied the Anti-SLAPP statute to obtain dismissal of plaintiffs' complaints. *Global Telemedia Int'l, Inc. v Doe 1* (CD Cal 2001) 132 F Supp 2d 1261 (negative comments about corporate performance of public telecommunications company posted on bulletin board protected as free speech); *Barrett v Rosenthal* (2006) 40 C4th 33, 41, 51 CR3d 55 ("newsgroups" where defamatory statements allegedly posted are "public forums" for purposes of the anti-SLAPP statute); *ComputerXpress, Inc. v Jackson* (2001) 93 CA4th 993, 113 CR2d 625 (disparaging Internet postings made in public forum for purposes of §426.16; website postings regarding publicly traded company represented speech by and for investors about matter of public interest, and were thus eligible for anti-SLAPP law protection). See also *Batzel v Smith* (9th Cir 2003) 333 F3d 1018, cert denied (2004) 541 US 1085 (vacating district court order denying anti-SLAPP motion). However, California courts have found that character statements about persons not in the public eye and statements about the performance of contractual obligations are not issues of public interest. *Dyer v Childress* (2007) 147 CA4th 1273, 1281, 55 CR3d 544.

Other states, including New York and Massachusetts, have enacted similar statutes. See NY CLS Civ R §§70-a, 76-a (anti-SLAPP statutes); NY CLS CPLR R 3211(g), R 3212(h) (motions for dismissal and summary judgment); Mass Gen Laws Ann Ch 231 §59H. Businesses or individuals who believe they are being unfairly targeted in lawsuits arising from positions taken on matters of public interest should refer to the anti-SLAPP statute for possible recourse.

© The Regents of the University of California

V. INTERNET COMPLAINT SITES

§20.26 A. Overview

Unhappy customers, disgruntled employees, and political activists have used Internet complaint sites, called gripe sites, to efficiently express their woes and complaints about individuals or businesses. To enable would-be commentators or other potentially interested parties to discover the gripe site, the site operator typically registers a domain name that is similar to the name of the target company or person.

Bally Total Fitness, Dunkin' Donuts, and Home Depot are among the companies that have been targets of gripe sites. Gripe sites are created to express frivolous claims as well as legitimate concerns. For example, a customer established a gripe site against Bally Total Fitness because of a billing dispute. A customer of Dunkin' Donuts used a gripe site to condemn the company for not carrying his low-fat creamer of choice. Political activists used a gripe site to criticize Home Depot for allegedly selling products made of wood from endangered species of trees. There are also complaint sites targeted at politicians, corporate executives, and celebrities. See *Bally Total Fitness Holding Corp. v Faber* (CD Cal 1998) 29 F Supp 2d 1161, discussed in §20.28. In October 2005 an arbitrator ruling on a Uniform Domain Name Dispute Resolution Policy (UDRP) claim brought by Homer TLC, Inc., the owner of the "Home Depot" and "The Home Depot" trademarks, refused to transfer the homedepotsucks.com domain name to Homer TLC. See *Homer TLC, Inc. v GreenPeople* (Oct. 25, 2005) Nat'l Arbitration Forum Case No. FA0508000550345, available at http://www.arb-forum.com/domains/decisions/550345.htm. For a discussion of the UDRP and the use of trademarks in domain names, see §20.30 and §§3.12-3.24.

Gripe sites may unfairly harm a business's reputation if the allegations are untrue. In addition, gripe sites may injure the target business economically if potential customers refrain from purchasing its services and products in reaction to the gripe site's content. Sections 20.27-20.32 discuss potential legal claims that may be made against the owner or operator of a complaint or gripe site. Because most lawsuits against complaint sites have been unsuccessful, however, targets of such sites should instead consider extrajudicial solutions to address the problem (see §20.32), or simply accept the fact that gripe sites have become commonplace.

© The Regents of the University of California

§20.27 B. Potential Causes of Action

As noted in §20.26, litigation has been generally ineffective in shutting down a complaint site established in good faith. Nonetheless, potential causes of action that may be brought against the complaint site operator include

- Defamation (see §20.28);
- Trademark infringement and dilution (see §20.29);
- Dilution of a famous mark (see §20.30); and
- Cybersquatting (see §§20.30-20.32).

© The Regents of the University of California

§20.28 1. Defamation

As discussed in §20.2, the plaintiff in an action for defamation must prove that a defamatory statement was made concerning another person, that the statement was published, at least negligently, to a third person, and, if the defamatory statement concerned a for-profit corporation, that the statement caused harm to the corporation's business. Restatement (Second) of Torts §§558, 561 (1977). A company that is the target of a gripe site would therefore have to prove that it was damaged as a direct result of the statements posted on the gripe site. Because consumer behavior can be influenced by many factors, however, it may be difficult to prove that a downturn in sales of a company's products or services was the result of a gripe site posting.

Moreover, the owner or operator of a gripe site may be difficult or impossible to identify. Companies targeted by gripe sites therefore sometimes try to pursue claims against ISPs because they usually can be identified and located more easily. ISPs, however, have generally not been held liable for actions of their subscribers (including owners or operators of complaint sites), because tort law generally does not impute liability merely for providing the forum in which defamation allegedly occurs. See generally §20.4. Further, the "Good Samaritan" provision of the Communications Decency Act (CDA) (47 USC §230(c)(1)), discussed in §§20.5-20.7, grants limited immunity to providers or users of interactive computer services from defamation liability on account of statements made by other providers or users. In addition, some gripe site postings, such as expressions of political views, may be protected under the First Amendment. See generally §20.15. Because it may be difficult for a business to prevail on a defamation claim, counsel is generally advised, except in the most egregious cases, to explore other remedies.

© The Regents of the University of California

§20.29 2. Trademark Infringement and Dilution

Gripe site cases often implicate trademark law. The first step in the analysis of whether a trademark infringement claim can be asserted against a complaint site is to determine whether the website is infringing on a protectable mark. For a more detailed discussion of trademark infringement and trademark dilution claims, see §§3.59-3.69. Some names of businesses or individuals names may not be eligible for trademark protection. See §3.31. Further, gripe sites may explain or describe a business only indirectly or suggestively, without using the actual name of the business, in which case trademark law may not apply.

Although trademark law may be implicated when gripe sites register domain names that consist of a company's name along with a derogatory word (*e.g.*, "starbucksucks.com"), courts are not always sympathetic to claims brought on trademark grounds against gripe sites operating in good faith. Under trademark infringement law, a company can claim that a domain name infringes its trademark rights if the defendant's use of the mark creates a likelihood of confusion, mistake, or deception among the relevant consumers. See 15 USC §1114; *Jews for Jesus v Brodsky* (D NJ 1998) 993 F Supp 282, aff'd without opinion (3d Cir 1998) 159 F3d 1351 (defendant's domain names, jewsforjesus.org and jews-for-jesus.com, were held to be confusingly similar to the plaintiff's trademark "Jews f*r Jesus" and its common law service mark "Jews for Jesus"). See §3.59. Arguably, however, consumers would not be confused if the domain name of a complaint site consists of a derogatory word next to the plaintiff's mark (like the "sucks.com" sites) or a different, contorted spelling of the mark. Indeed, in *Taubman Co. v Webfeats* (6th Cir 2003) 319 F3d 770, the Sixth Circuit found just such a lack of confusion persuasive and rejected the plaintiff's claim that the defendant's "sucks site," http://www.taubmansucks.com, infringed the plaintiff's trademark in the Taubman name. According to the court, "in contrast to [a site that merely uses the trademark of another], 'taubmansucks.com' removes any confusion as to source." 319 F3d at 778. The Sixth Circuit held that the defendant's use of the "sucks site" was "purely an exhibition of Free Speech, and the Lanham Act is not invoked." 319 F3d at 778.

A gripe site may also be liable for trademark dilution under the Federal Trademark Dilution Act of 1995 (15 USC §1125). For more detailed discussion of trademark dilution claims, see §§3.64-3.67. The activities of the gripe site may be protected, however, under 15 USC §1125(c)(3), which exempts from liability (1) fair use of a famous mark, (2) noncommercial uses of a mark, and (3) all forms of news reporting and commentary. Because most gripe site operators do not receive an economic benefit from the site, their actions would typically fall under the "noncommercial uses of a mark" exemption, 15 USC §1125(c)(3)(C). See *Bally Total Fitness Holding Corp. v Faber* (CD Cal 1998) 29 F Supp 2d 1161 (website containing mark BALLY with word "sucks" printed over it and stating "Bally Total Fitness Complaints! Un-Authorized" was protected because defendant did not gain economically from site). But see *Jews for Jesus v Brodsky, supra* (defendant benefited economically from site because it contained hyperlink to commercial site defendant operated). This analysis has been held to apply when a defendant is operating a gripe site that uses a plaintiff's trademark without the addition of "sucks" or anything similar, as long as the defendant is not using the site to pursue commercial gain. See *TMI, Inc. v Maxwell* (5th Cir 2004) 368 F3d 433 (dilution liability requires finding that defendant accused of dilution made commercial use of mark).

© The Regents of the University of California

3. Cybersquatting: Federal and State Law

§20.30 a. UDRP

The Uniform Domain Name Dispute Resolution Policy (UDRP) of the Internet Corporation for Assigned Names and Numbers (ICANN) establishes an arbitration procedure to resolve claims that a domain name infringes on a trademark owned by another. For a more detailed discussion of UDRP, see §§3.12-3.21. Although the UDRP was mainly directed at cybersquatters, it may also be applied to gripe sites under certain circumstances. A UDRP arbitration panel may cancel, transfer, or otherwise change a domain name if the complainant can prove the following (UDRP ¶4(a)):

- The challenged domain name is identical or confusingly similar to a trademark or service mark in which the claimant has rights;
- The respondent domain name holder has no rights or legitimate interest in the domain name; and
- The domain name has been registered and is being used in bad faith.

See §3.12. In assessing whether a domain name is being used in bad faith, a panel considers several factors, including whether the domain name was registered with the purpose of later selling the name to the owner of the trademark, whether the domain name was registered primarily to disrupt the business of a competitor, and whether the domain name was registered with the intent to attract users for commercial benefit by creating a likelihood of confusion with the original trademark. See ICANN's Uniform Domain Name Dispute Resolution Policy at http://www.icann.org/en/udrp/udrp-policy-24oct99.htm. See also §§3.12-3.21.

In certain circumstances, UDRP arbitration panels have found that an individual person has trademark rights in his or her own name, particularly when the individual's name provides commercial value to him or her in a manner akin to a trademark. See *Julia Fiona Roberts v Russell Boyd,* WIPO Case No. D2000-210 (finding that actress Julia Roberts had common law trademark rights in her name sufficient to make out claim under UDRP). But see *Israel Harold Asper v Communication X Inc.,* WIPO Case No. D2001-0540 (because complainant Israel Harold Asper, notable Canadian businessman, author, lawyer, politician, and philanthropist, had never used his name "for the purpose of merchandising or other commercial promotion of goods or services," it was not source identifier protectable by trademark law and defendant could not be prohibited from using domain names izzyasper.com, izzyasper.net, and izzyasper.org); *Falwell & Anor v Cohn & Ors,* WIPO Case No. D2002-0184 (name "Jerry Falwell," although well known, had not been used in trademark sense, therefore was not protected by trademark law). World Intellectual Property Organization (WIPO) cases are available at http://arbiter.wipo.int/domains/decisions.

Decisions of UDRP panels regarding names of politicians are somewhat varied. See, *e.g., Mark Warner 2001 v Mike Larson,* Nat'l Arbitration Forum Case Case No. FA0009000095746, Nov. 15, 2000, available at http://www.arb-forum.com/domains/decisions/95746.htm (although as former U.S. Senate candidate and presumptive candidate for governor of Virginia, complainant had common law trademark rights in "Mark Warner," he was denied relief because he did not show evidence that respondent acted in bad faith when he registered domain name markwarner2001.com). See also *Friends of Kathleen Kennedy Townsend v B.G. Birt*, WIPO Case No. D2002-0451 (relief denied because complainant organization lacked common law trademark rights in "Kathleen Kennedy Townsend").

Generally, UDRP panels have held names of celebrities and athletes to be trademarks. See *Helen Folsade aka Sade v Quantum Computer Servs. Inc.,* WIPO Case No. D2000-0794 (respondent prohibited from "trading on the Complainant's goodwill" by using domain name "sade.com" because singer Sade had established common law trademark rights in "Sade" by using it as stage-name and to "distinguish her goods and services as a singer, songwriter, performer and recording artist"). See also *Roberts v Boyd,* WIPO Case No. D2000-0210; *Springsteen v Burgar,* WIPO Case No. D2000-1532. For names of athletes as trademarks, see, *e.g., Marino v Video Images Prods.,* WIPO Case No. D2000-0598.

NOTE: a trademark holder who is unsuccessful in a UDRP proceeding may still bring a lawsuit under the Anticybersquatting Consumer Protection Act (ACPA), discussed in §§3.22-3.24, 20.31.

© The Regents of the University of California

§20.31 b. Anticybersquatting Consumer Protection Act

The Anticybersquatting Consumer Protection Act (ACPA) (Pub L 106-113, 113 Stat 1501A), principally codified in 15 USC §1125(d), is discussed more fully in §§3.22-3.24. A violation of the ACPA occurs when (15 USC §1125(d)):

(a) a domain name is identical or confusingly similar to a mark that was distinctive when the domain name was registered, or is identical or, confusingly similar to, or dilutive of, a mark that was famous when the domain name was registered; and

(b) the defendant registers, traffics in, or uses the domain name with a bad faith intent to profit.

The utility of the ACPA as a basis for a claim against a gripe site operator is limited because gripe site operators usually do not have a "bad faith intent to profit." See 15 USC §1125(d); §20.28. Although the ACPA provides a remedy for use of a living person's name as a domain name even if that person's name is not a protectable mark (see 15 USC §1129; §§3.22, 20.29), the plaintiff must show that the defendant had a specific intent to profit from selling the domain name for financial gain to a third party. Thus, if a gripe site operator offers to sell its domain name to the target business in the manner of a cybersquatter, the ACPA may be implicated. Absent some commercial motive on the part of the gripe site operator, however, a claim under the ACPA will be difficult to maintain. In addition, because gripe sites (and in particular, "sucks" sites) have been held not to infringe the trademarks of those to whom the gripes are directed, the ACPA may not be available to force transfer of a gripe site domain name away from the gripe site operator. See *Lucent Techs., Inc. v Lucentsucks.com* (ED Va 2000) 95 F Supp 2d 528, 536 (noting in dicta that "a successful showing that lucentsucks.com is effective parody and/or a cite [sic] for critical commentary would seriously undermine the requisite elements for the causes of action at issue in this case").

© The Regents of the University of California

§20.32 c. California's Anticybersquatting Statute

California has also enacted an anticybersquatting statute (Bus & P C §§17525-17528), which protects the names of living or deceased persons and eliminates the ACPA's requirement of a specific intent to profit from selling the domain name. A significant difference between the California statute and the ACPA is that the California law protects all personal names from cyberpiracy, not just "famous" names. The statute requires a showing of a bad faith intent to register, traffic in, or use a domain name that is identical or confusingly similar to the personal name of another living person or deceased personality, without regard to goods or services of the parties. Bus & P C §17525. The California statute is therefore not addressed to trademarks. The statute sets forth eight factors to be considered when determining whether a bad faith intent exists, including (Bus & P C §17526(d)):

The legitimate noncommercial or fair use of the person's or deceased personality's name in an Internet web site accessible under the domain name by the person alleged to be in violation of this article.

Thus, for example, a gripe site operator might defend a claim under the California anticybersquatting statute by asserting that its use of the person's name was "fair use" under Bus & P C §17526(d).

© The Regents of the University of California

§20.33 C. Practical Solutions

Because the legal remedies described in §§20.27-20.32 may prove to be ineffective remedies against gripe sites, the following practical solutions should be considered to prevent such sites from operating.

Businesses should consider registering variations of their domain names ("secondary domain names"), such as "[name]sucks.com," "[name]stinks.com," or "boycott[name].com," to foreclose use of those name variants by gripe site operators. In addition, all suffixes or top level domain names (such as .COM, .BIZ, and .ORG) available for the secondary domain names should be registered. For discussion of domain name registration, see §§3.2-3.3, 3.6. See ICANN's website at http://www.icann.org/tlds for a list of top level domain names. Some businesses have taken the additional step of registering the names of their officers, directors, and other representatives to whom the public may have access, or whose names may be publicly available in connection with the business's operation. If a gripe site operator cannot register a domain name that is similar to the person or business it would like to post complaints about, then the operator will be forced to register a dissimilar name, which should reduce the number of potential visitors to the gripe site.

Additional approaches that targeted businesses may wish to consider include:

- Monitoring complaints made on the gripe site so that the targeted company can contact the gripe site owner to express interest in resolving the dispute.
- Providing a link on the company's own website to enable individuals to complain directly to the company.
- Sending coupons or free products to pacify unhappy customers and quell their complaints. Some businesses have found this approach successful; the genesis of many gripe sites is a failure to be responsive to customer complaints.
- Rebutting claims made on the complaint site on the company's own website.
- Sending a letter requesting the gripe site operator to cease using the company's name or a person's name in connection with the site. For a sample form of cease and desist letter, see §3.63. Note that cease and desist letters are often posted on the gripe site along with further inflammatory comments, which may spur further complaints about the business and make the problem worse.
- Purchasing the complaint site from the operator.

© The Regents of the University of California

VI. INSURANCE ISSUES FOR ONLINE BUSINESSES

§20.34 A. Introduction

As e-commerce develops as a key source of revenue for traditional "brick and mortar" companies as well as Internet-based businesses, and Internet usage for intercompany communications and day-to-day business transactions continues to increase, Internet websites and stored electronic data have become extremely valuable corporate assets. Business interruptions resulting from inaccessible or malfunctioning websites or lost data can have serious economic implications. Moreover, conducting business online may create liabilities to third parties, *e.g.,* by passing a virus to a third party, infringing third party intellectual property rights, or breaching privacy obligations.

Faced with losses or third party claims, companies may look to their traditional comprehensive general liability insurance policies for recovery. Policy holders should consider the scope of coverage for their Internet-related activities under their existing insurance policies, particularly in light of recent changes to standard policy forms (see §20.41) and developing case law. In addition, when engaging a third party to provide services in connection with an Internet business, understanding the recourse available under the service provider's insurance coverage is an important element of assessing risk and evaluating vendors. While the analysis of any particular claim must be reviewed based on the coverage actually in place and the specific facts involved, §§20.35-20.42 provide a general overview of the issues and case law on insurance coverage for Internet-related activities. For an overview of insurance issues facing online businesses, see Rowen, *Avoiding Bad Days For Risk Managers: Insurance For Internet Related Risks*, posted at the State Bar of California website at http://www.calbar.ca.gov/state/calbar/calbar_generic.jsp?sImagePath=Business-Law_Insurance.gif&sCategoryPath=/Home/Attorney%20Resources/Sections/Business%20Law/Standing%20Committees/Insurance%20Law&sHeading=Insurance%20for%20Internet-Related%20Risks&sFileType=HTML&sCatHtmlPath=html/Business-Law_Cmtes_Insurance_Articles_Avoiding_Bad_Days.html.

© The Regents of the University of California

§20.35 B. Commercial Form General Liability Insurance

Of the two main types of liability insurance, the commercial form general liability policy is the primary form of coverage for business owners seeking to use insurance as a tool in their asset protection planning. Known as "third party" coverage, liability insurance covers personal injury and property damages that the insured causes to other persons; it does not protect property owned by the insured. Policies covering the insured's own property are known as property policies or "first party" coverage.

Commercial form general liability (CGL) insurance covers all liability for personal injuries or property damage caused to other persons, unless specifically excluded. It often provides coverage for defamation claims stemming from the advertising activities of the policy holder. A policy holder is advised to review all of the exclusions in order to ascertain the true scope of coverage.

For example, CGL insurance covers damages to another person's property only if the property is "tangible" or the damage "physical." Therefore, a threshold issue is whether the property is in fact "tangible" or susceptible to "physical" harm. This issue is particularly relevant to electronic data and items of intellectual property. Thus, a company that provides computer hardware, software, or programming services should determine whether its standard CGL policy includes appropriate coverage for its activities. If the policy does not include the desired coverage, the company should consider requesting an endorsement that includes the coverage or else purchasing a separate, specialized liability policy.

© The Regents of the University of California

§20.36 1. Loss of Tangible Property: Is Computer Data "Tangible Property?"

Regarding coverage for property damage, courts have split on the question of whether and to what extent computer and data losses should be covered by commercial general liability insurance. A majority of courts that have looked at the question have held that where there is no loss of or damage to tangible property, there is no insurance coverage under CGL policies. The loss of electronic data does not involve the loss of tangible property. See, *e.g.*, *Magnetic Data Inc. v St. Paul Fire & Marine Ins. Co.* (Minn 1989) 442 NW2d 153 (while holding that "control of property" exclusion barred coverage for insured's inadvertent erasure of customer's disk, court also noted that general liability policies do not cover damages to intangible property). But see *Retail Sys., Inc. v CNA Ins. Cos.* (Minn App 1991) 469 NW2d 735 (computer data recorded on lost tape was merged with tape; therefore, loss of tape was covered as loss of tangible property).

In *America Online, Inc. v St. Paul Mercury Ins. Co.* (ED Va 2002) 207 F Supp 2d 459, aff'd (4th Cir 2003) 347 F3d 89, AOL users alleged that downloading and using AOL's new software damaged their computers systems by disrupting Internet and local area network connections, causing system instability, crashing computers, and corrupting files. The first issue was whether computer data, software, and systems were tangible property under AOL's CGL policy. "Tangible" was not defined in the policy, so the court looked to the plain meaning of the word. Black's Law Dictionary defines "tangible" as "[H]aving or possessing physical form. Capable of being touched and seen; perceptible to the touch; tactile." Black's Law Dictionary (6th ed 1990). Webster's Third New International Dictionary also defines "tangible" as "capable of being touched." Webster's Third New International Dictionary (1993). See 207 F Supp 2d at 467. The court found that computer data can be transmitted and stored in a variety of ways, but none of them rendered the data capable of being "touched" like a chair or a book. The court reasoned that electrical impulses that carry computer data are imperceptible to the human eye and can only be perceived with the help of a computer. 207 F Supp 2d at 468. The court held that because the policy covered only damage to tangible property, no coverage existed under AOL's CGL policy for the damages caused by its software program.

In *Avery Dennison Corp. v Allendale Mut. Ins. Co.* (9th Cir 2002) 310 F3d 1114, the Ninth Circuit held that trade secrets do not qualify as "tangible property." Plaintiff Avery Dennison had purchased an insurance policy with special coverage for crime, including loss or damage to "Covered Property" caused by employee dishonesty. "Covered Property" was defined, in part, as "tangible property … that has intrinsic value." 310 F3d at 1116. The plaintiff made a claim under the policy after an employee sold trade secrets to a competitor. Rejecting the plaintiff's claim for coverage, the court held that "'[t]angible property' is not an ambiguous term, and its meaning is sufficiently clear that an expectation that it would cover trade secrets is not reasonable." 310 F3d at 1117.

Supporting the contention that computer data is tangible property, the court in *American Guar. & Liab. Ins. Co. v Ingram Micro, Inc.* (D Ariz, Apr. 19, 2000, No. CIV 99-185 TUC ACM) 2000 US Dist Lexis 7299, held that a power outage qualified as "physical loss" under an insurance policy. The court found that "'physical damage' is not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality." 2000 US Dist Lexis 7299, *6.

© The Regents of the University of California

§20.37 2. Loss of Tangible Property: Has There Been a "Loss"?

Courts have denied recovery against insured companies by finding no actual loss of property but instead only a loss of some benefit related to the property. In *St. Paul Fire & Marine Ins. Co. v National Computer Sys., Inc*. (Minn App 1992) 490 NW2d 626, a case involving data in hard copy (not in electronic form), the insured used photocopies of its competitor's confidential pricing information obtained from a former employee of the competitor. The insurer argued that under *Magnetic Data Inc. v St. Paul Fire & Marine Ins. Co.* (Minn 1989) 442 NW2d 153, the loss of data was a loss of intangible property and therefore uninsured. The court reasoned, however, that although the data had been misappropriated in tangible form, the information it represented had not been lost or damaged because the owner of the data retained the information in its original (tangible) form. Therefore, there was no loss of data, but only the loss of exclusive use of the information. There was no coverage because there was no damage to or loss of use of tangible property, only an injury to the company's exclusive right to use the property.

The distinction between actual loss of data and loss of some benefit related to the data is important. In *Peoples Telephone Co. v Hartford Fire Ins. Co*. (SD Fla 1997) 36 F Supp 2d 1335, the court relied on *St. Paul Fire & Marine Ins. Co. v National Computer Sys., Inc., supra,* to hold that an insurance policy protecting against employee theft did not cover losses sustained when an employee of a cellular telephone service provider disclosed access codes that enabled noncustomers to use the telephone service. The court held that the case did not involve a loss of "tangible property" but merely the loss of the economic value of the access codes, which the court concluded was intangible. As in *National Computer Systems,* the loss arose not out of the loss of data, but from an inability to restrict the use of the data by others.

© The Regents of the University of California

§20.38 3. "Physical Loss or Damage"

The question of whether loss of computer data can be a "physical loss or damage" to property was addressed in *American Guar. & Liab. Ins. Co. v Ingram Micro, Inc.* (D Ariz Apr. 19, 2000, No. CIV 99-185 TUC ACM) 2000 US Dist Lexis 7299. Ingram Micro suffered damage when a short in an internal fire alarm panel shut down the company's main data center, which handled orders for its products. As a result, Ingram's mainframe computers lost all programming information and configurations. Ingram was able to restore the network and reload the lost data but lost sales and revenues. Once the computers were reprogrammed, they functioned normally. Ingram made a business interruption claim under its general liability policy. Ingram's policy insured against "all risks of direct physical loss or damage from any cause, howsoever or wheresoever occurring" for "real and personal property." 2000 US Dist Lexis 7299 at 3. The insurance company denied coverage, arguing that the computers were not "physically damaged" because they were able to function after their programming and data were restored. The court disagreed, finding that "'physical damage' is not restricted to the physical destruction or harm of computer circuitry, but includes loss of access, loss of use, and loss of functionality." 2000 US Dist Lexis 7299 at 6. Therefore, the damage caused by the power outage was "property damage" under the insurance policy. In reaching its conclusion, the court analogized to the Federal Computer Fraud and Abuse Act (18 USC §1030), which defines computer damage broadly to include impairment to availability of data or alteration of data.

The Ninth Circuit refused to hear an appeal in *Ingram Micro,* thus leaving the *Ingram Micro* decision in place. It does not appear that any other court has adopted the *Ingram Micro* definition of "physical damage," and a more recent case from a federal district court in Oklahoma reached the opposite result. See *State Auto Prop. & Cas. Ins. Co. v Midwest Computers & More* (WD Okla 2001) 147 F Supp 2d 1113 (claim that computer servicing company destroyed information stored on customers' hard drives not covered because information was intangible; however, claim for loss of use of computer was covered as property damage). The *Ingram Micro* holding has been cited on at least one recent occasion in a somewhat analogous but not equivalent context. See *America Online, Inc. v National Health Care Discount, Inc.* (ND Iowa 2000) 121 F Supp 2d 1255, 1274 n18 (relying on *Ingram Micro* to support its holding that diminished network capacity caused by large volume of spam e-mail constituted "damage" for purposes of Computer Fraud and Abuse Act (18 USC §1030)).

© The Regents of the University of California

§20.39 4. Intellectual Property Infringement

The broad coverage available to insureds under commercial form general liability (CGL) insurance policies may or may not extend to intellectual property infringement claims, especially those relating to trademark and copyright infringement. As explained below, CGL insurance coverage often does not extend to intellectual property claims based on patent infringement absent specific additional coverage, which much be procured at extra cost. Where available under CGL policies, coverage for intellectual property infringement claims typically falls within the "advertising injury" portion of the policy. To establish coverage under the advertising injury provisions, however, the insured must show that the claim arising from alleged copyright or trademark infringement or trade secret misappropriation relates to the insured's advertising activities. See *Delta Computer Corp. v Walter J. Frank, Inc.* (5th Cir 1999) 196 F3d 589. In order to determine whether the insurer has a duty to defend or indemnify the insured under an "advertising injury" provision, some courts, as acknowledged in *State Farm Fire & Cas. Co. v Steinberg* (11th Cir 2004) 393 F3d 1226, 1231, have adopted a three-part test:

- The claim must have a recognizable advertising injury.
- The infringing party must have participated in advertising activity.
- A causal connection exists between the advertising activity and the advertising injury.

Other courts have held that there is no advertising injury coverage for misappropriation of trade secrets because the act of misappropriation occurs before any promotion or advertising activity related to the trade secret. *Winklevoss Consultants, Inc. v Federal Ins. Co.* (ND Ill 1998) 991 F Supp 1024. Similarly, courts have found that patent infringement cannot be committed in the course of advertising activities, therefore there is no insurance coverage for such claims. *Gencor Indus., Inc. v Wausau Underwriters Ins. Co.* (MD Fla 1994) 857 F Supp 1560; *Aetna Cas. & Sur. Co. v Superior Court* (1993) 19 CA4th 320, 23 CR2d 442. One court held that there was no insurance coverage for patent infringement even where the party bringing the action relied on the infringing party's use of press releases, brochures, and catalogs to advertise the infringing product. *FileNet Corp. v Chubb Corp.* (NJ App 1999) 735 A2d 1170. CGL coverage, therefore, while providing broad coverage for a range of liabilities, does have limitations in certain areas of intellectual property coverage, and companies at risk of patent or trade secret infringement claims are advised to make sure that they understand the scope (and the limits) of the insurance coverage that they have purchased.

© The Regents of the University of California

§20.40 C. Business Interruption Coverage

A policyholder's property insurance normally covers repair or replacement of damaged property but does not protect the insured against consequential damages. Business interruption coverage is intended to fill that gap. The purpose of business interruption coverage is to protect the insured against a loss of income if it suffers a loss that causes it to suspend operations. Business interruption coverage is often linked to a property policy and applies only if the suspension of operations is caused by direct physical loss or damage to property. The loss typically must be caused by a "covered loss" as defined under the policy.

Because many companies doing business on the Internet also have "brick and mortar" components, one issue is whether a suspension in operations of the Internet-based side of their business will trigger business interruption coverage. Shutdown of a web site may result in only partial disruption of a business if it employs multiple distribution channels for its products.

In *Home Indem. Co. v Hyplains Beef* (D Kan 1995) 893 F Supp 987, aff'd without opinion (10th Cir 1996) 89 F3d 850, the insured purchased a computer system to control operations at its beef processing plant. Immediately after installation, the computers malfunctioned and production slowed. The insured argued that the loss of productivity constituted a "suspension" of its operations. The court noted that although the term "suspension" was not defined in the policy, it was not ambiguous; therefore, it must be given its plain and ordinary meaning. The court determined that the "common understanding of the term 'suspension' [is] a temporary, but complete, cessation of activity." 893 F Supp at 991. The court found that a mere loss of productivity did not constitute a suspension of the insured's operations within the meaning of the policy. Accordingly, the insured could not recover the profits it lost as a result of the computer failure.

© The Regents of the University of California

§20.41 D. Industry Response

The insurance industry has reacted to coverage issues by introducing new endorsements and other policy language that exclude certain e-commerce-related risks. In 2001, the Insurance Services Office (ISO), the industry organization that proposes standard insurance policy language, revised its commercial general liability forms to limit coverage for business activities over the Internet and other computer networks. Insurers who use proprietary forms are doing the same.

As discussed in §20.36, one of the key issues for coverage of an e-commerce-related loss under standard insurance policies is whether electronic data or computer data constitutes "tangible property." The ISO has added the following sentence to the definition of "property damage" in the CGL form: "For the purposes of this insurance, electronic data is not tangible property." Also, according to the new form, "electronic data" encompasses

information, facts, or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.

NOTE: With the new definition of "property damage" in the ISO's model CGL form, transmission of a virus would not trigger coverage because it would ordinarily not cause physical injury to tangible property.

Insurance companies are not required to adopt the ISO language; they individually decide what language to include in their policies. The proposed ISO language, however, indicates that the insurance industry is attempting to deter further litigation over whether standard CGL policies cover damages related to Internet risks.

Another change is in the area of advertising liability coverage. The ISO model form now reflects an exclusion from coverage for certain Internet-related business activities such as website design services, Internet service providers, Internet search services, electronic chat rooms, and bulletin boards. The definition of what is an "advertisement," however, now includes "material placed on the Internet or on similar electronic means of communication" such as Internet ad banners. The new definition classifies as an advertisement only that portion of a website that relates to the insured's goods or services "for the purposes of attracting customers or supporters."

© The Regents of the University of California

§20.42 E. Conclusion

All companies doing business on the Internet should review their existing insurance coverage carefully to determine whether their policies provide coverage for claims that might arise from their online business activities. Recently issued policies may contain specific exclusions for losses involving electronic data, software, or computer programs. If there are gaps in coverage, a company may be able to purchase a separate policy or endorsement specifically designed to cover potential claims arising from online business activities. These policies, however, vary greatly in coverage and premium cost. Moreover, the underwriting process for these policies can be difficult. Insurers may require the company to complete a detailed application about its website, requesting information on the average page views per month, the content of the site, whether personal data regarding site visitors is collected, whether e-commerce transactions occur at the site, whether the site includes hyperlinks, message boards, or advertisements, whether the site uses proprietary software, and whether it has a posted privacy policy. Many insurance companies require that a consultant review the site's security features before placing the insurance. Companies that engage third parties to perform Internet-related services should determine whether the service provider has adequate insurance coverage for potential liability to the company if the service provider fails to perform.

© The Regents of the University of California

20A

Discovery of Electronically Stored Information

Alexander H. Lubarsky

I. INTRODUCTION §20A.1

II. MANAGING ELECTRONICALLY STORED INFORMATION BEFORE LITIGATION
- A. Retention of ESI
  - 1. Regulatory Obligations §20A.2
  - 2. In Absence of Statute or Regulation §20A.3
- B. Document Retention Policies §20A.4
- C. Special Problems Concerning E-mail §20A.5

III. FEDERAL RULES ON ELECTRONIC DISCOVERY §20A.6
- A. Rule 16: Scheduling Orders §20A.7
- B. Rule 26: General Discovery Provisions; Duty of Disclosure
  - 1. Initial Voluntary Disclosure §20A.8
  - 2. "Clawback" of Privileged Material §20A.9
  - 3. Meet-and-Confer Requirements §20A.10
  - 4. Safe Harbor if ESI Not Reasonably Accessible §20A.11
- C. Rule 33: Interrogatory Responses §20A.12
- D. Rule 34: Production of Documents and Things
  - 1. Rule 34(a): Inspection, Copying, Testing, and Sampling §20A.13
  - 2. Rule 34(b): Specifying Format for Production §20A.14
- E. Rule 37: Safe Harbor for Routine Deletion §20A.15
- F. Rule 45: Response to Subpoenas §20A.16

IV. CALIFORNIA LAW
- A. Rules of Court §20A.17
- B. Electronic Discovery Act §20A.18
  - 1. ESI From Sources Not Reasonably Accessible §20A.18A
  - 2. Safe Harbor for Lost Information §20A.18B
  - 3. Disclosure of Privileged Information §20A.18C
  - 4. Form of Production §20A.18D
  - 5. Court-Imposed Limits on Production §20A.18E

V. ADVANCE PREPARATION FOR DISCOVERY OF ESI
- A. ESI Survey and Retention Policy §20A.19
- B. Identifying Key Personnel §20A.20

VI. RETENTION OF ESI WHEN LITIGATION IS PENDING
- A. Notice of Litigation §20A.21
- B. Duty to Preserve Evidence §20A.22
- C. Legal Hold Letter to Client
  - 1. Legal Holds §20A.23
  - 2. Form: Legal Hold Letter to Client §20A.24
- D. Litigation Hold Letter To Opponent
  - 1. Litigation Holds §20A.25
  - 2. Form: Litigation Hold Letter to Opponent §20A.26
- E. Manner of Preservation §20A.27
- F. Sanctions for Failure to Preserve §20A.28

VII. DISCOVERY OF ESI
- A. Identifying Data for Discovery
  - 1. Need to Understand ESI Infrastructure §20A.29
  - 2. Drafting a Request for Production §20A.30

B. Collecting Data
1. Defensible Collection Strategies §20A.31
2. Paper-Based Versus Electronic Production §20A.32
3. Forensic Data Professionals §20A.33
4. Electronic Data Discovery Software §20A.34
5. Risks in ESI Collection §20A.35
6. Metadata §20A.36
7. Forensic or Mirror Images §20A.37
8. Right to On-Site Inspection §20A.38
C. Form of Production §20A.39
1. Production in Native Format §20A.40
2. Production of Image Files §20A.41
a. Copying Electronic Files §20A.42
b. Handling Metadata §20A.43
D. Privileged Information §20A.44
E. Federal Rule of Evidence 502 §20A.44A
F. Data Processing, Storage, and Review
1. De-Duplication §20A.45
2. Litigation Support Platforms §20A.46
3. Hosting §20A.47
4. Data Security §20A.48
G. Costs of E-Discovery §20A.49

© The Regents of the University of California

§20A.1 I. INTRODUCTION

It is estimated that over 97 percent of all business records are now created and maintained in electronic format and that the number of e-mail messages worldwide now exceeds 35 billion per day. It is therefore not surprising that the majority of documentary evidence requested, produced, and introduced in the course of litigation now consists of electronic records created and stored in computers, personal digital assistants (PDAs), cell phones, and other electronic devices. Moreover, information that may be germane to a legal dispute can now be found across a vast new array of social networking sites such as Facebook, Twitter, and MySpace. Attorneys and even paralegals must understand how electronically stored information (ESI) can be identified, located, and retrieved intact. Courts are increasingly required to consider the scope of e-discovery and the procedures used for identifying and collecting ESI. Courts are evaluating the legitimacy of methods used to preserve and produce ESI and deciding how parties should bear the costs of e-discovery, and the Federal Rules of Civil Procedure have been revised to expressly address ESI. Harsh sanctions may be imposed on both the attorney and the client who do not follow the rules of evidence and procedure governing electronic discovery.

This chapter surveys the retention, review protocols, and ultimate production of ESI within the discovery process, and the evolving principles that govern it for attorneys on both sides of a discovery request. For further discussion of e-discovery, see California Civil Discovery Practice, chap 4 (4th ed Cal CEB 2006). See also the CEB webcast titled "New Strategies for Winning the Electronic Document Production War," available at http://ceb.com.

© The Regents of the University of California

II. MANAGING ELECTRONICALLY STORED INFORMATION BEFORE LITIGATION

A. Retention of ESI

§20A.2 1. Regulatory Obligations

In certain regulated industries, such as health care, securities, and banking, statutes and regulations set forth requirements for preservation of records (including electronic records) that could prove useful in later audits, investigations, or litigation. Federal legislation with provisions addressing data preservation and storage include the following:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub L 104-191, 110 Stat 1936) Security Rule (45 CFR Pts 160, 162, and 164), which defines the physical and technical safeguards that protect patient information in electronic form;
- Sarbanes-Oxley Act of 2002 (Pub L 107-204, 116 Stat 745), which, among other things, directs accountants to maintain certain corporate audit records and review work papers for a period of 5 years from the end of the fiscal period during which the audit or review was concluded, and institutes new penalties for document alteration or destruction done with an intent to impede or obstruct a federal investigation; and
- Gramm-Leach-Bliley Financial Modernization Act of 1999 (Pub L 106-102, 113 Stat 1338), which regulates the handling of nonpublic consumer information by financial institutions.

In a case involving investment bank Morgan Stanley, a Florida trial court found that the defendant's repeated failure to produce requested e-mails and other documents shifted the burden of proof on the plaintiff's allegations of securities fraud. *Coleman (Parent) Holdings, Inc. v Morgan Stanley & Co.* (Fla Cir Ct, Mar. 1, 2005, No. 502003CA005045XXOCAL) 2005 WL 679071, rev'd on other grounds (Fla App 2006) 955 So2d 1124. The discovery problems continued for a year, and the court found that Morgan Stanley had acted in bad faith by overwriting e-mails in direct violation of 17 CFR §240.17a-4, which requires securities broker-dealers to preserve e-mails and other records for specified periods of up to 6 years. The court granted a partial default judgment in the amount of $1.5 billion against the firm. In early 2006, the Securities and Exchange Commission fined Morgan Stanley $15 million for its failure to preserve e-mails in violation of SEC rules. In March 2007, Morgan Stanley persuaded a Florida appeals court to reverse the $1.5 billion sanction. Although the court found that Coleman failed to prove entitlement to damages in the original trial, the court's findings pertaining to the discovery shortcomings that resulted in sanctions were not disturbed on appeal. *Morgan Stanley & Co. v Coleman (Parent) Holdings, Inc.* (Fla App 2007) 955 So2d 1124.

© The Regents of the University of California

§20A.3 2. In Absence of Statute or Regulation

Outside of the regulated industries, what constitutes an appropriate electronic document retention policy for a commercial business if no litigation is reasonably foreseeable is often not clear and may depend on many factors. A company's need to save data and its need to delete data permanently represent competing objectives. The trend in computer engineering is to make data easier to save and therefore harder to erase. (In general, computers discard stored information by "overwriting" that information with new information. A keyboard "delete" command identifies files stored in the hard drive that are available for overwriting. Even if a file is overwritten, however, forensic tools may still be able to recover old data.) As it becomes easier and less costly to store large amounts of ESI, the amount of data created and stored by the average business has increased exponentially; yet, the task of managing it so that it can be indexed and retrieved easily when necessary can be costly and complicated.

It is impractical and cost prohibitive for an average business to keep all ESI generated, and, except as discussed in §20A.2, there is no authority that mandates preservation of every electronic record if litigation is not on the horizon. As Judge Scheindlin stated in *Zubulake v UBS Warburg LLC* (SD NY 2003) 220 FRD 212, 217, there is no duty to "preserve every shred of paper, every e-mail or electronic document, and every backup tape.... Such a rule would cripple large corporations."

Both the Federal Rules of Civil Procedure, amended in 2006 to address ESI issues (see §§20A.6-20A.16), and the California Electronic Discovery Act (Stats 2009, ch 5) (see §§20A.17-20A.18E) provide for a court to limit the duty of production of data where "the likely burden or expense of the proposed discovery outweighs the likely benefit." CCP 1985.8(h)(4). See also Fed R Civ P 26(b)(2)(B) ("A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost").

Traditionally, production of backup media such as tapes and cartridges that require restoration to a usable format before the data is manageable by counsel was less likely to be required. However, this data has become more easily accessible now that "do it yourself"' tape restoration software and greater availability of tape restoration vendors make it possible to restore most data-backup tapes and cartridges easily and cost effectively. Because of this trend, the courts are less inclined to relieve a party of its duty to preserve data, especially when the probative value outweighs the increasingly diminishing burden associated with its preservation, identification, collection, and production.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/20A Discovery of Electronically Stored Information/§20A.4 B. Document Retention Policies

§20A.4 B. Document Retention Policies

Well in advance of reasonably foreseeable litigation, counsel should advise the client to design and implement a reasonable plan for routine electronic data storage, preservation, and destruction. As the U.S. Supreme Court has stated, under ordinary circumstances, it is not wrongful or improper for a company manager to instruct his or her employees to comply with a valid document retention policy. *Arthur Andersen LLP v U.S.* (2005) 544 US 696, 704, 161 L Ed 2d 1008, 1017, 125 S Ct 2129. New Fed R Civ P 37(e) provides a safe harbor from potential sanctions for loss or alteration of ESI, by providing in part:

> [a]bsent exceptional circumstances, a court may not impose sanctions… on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.

See also §20A.15. Because there is no single standard regarding the length of time that businesses are required to keep ESI, the amount of time specified by a retention policy may be a matter of controversy. Businesses should be aware of the data-saving standards that other businesses within the same industry are using. Data maintained within certain industries such as finance, health care, pharmaceutical, and tobacco are highly regulated by specific legislative directives. Counsel should research those standards to assure that their clients adhere to them as evidence that the client's handling of ESI has been routine, in good faith, and in accordance with commercial standards prevalent in—and regulations governing—the industry.

Federal rules require parties to cooperate in defining legitimate discovery needs and limiting the high costs of electronic discovery. *Mancia v Mayflower Textile Servs*. Co. (D Md 2008) 253 FRD 354, 357. In *William A. Gross Constr. Assocs., Inc. v American Mfrs. Mut. Ins. Co.* (SD NY 2009) 256 FRD 134, the court noted counsels' duty to cooperate and found that attorneys seeking discovery of e-mails have an obligation to craft appropriate keywords carefully, with input from the ESI's custodians regarding the words and abbreviations they use, in order to eliminate "false positives."

NOTE: Many law firms have added e-discovery partners and practice groups and have turned to compliance consulting as a way to provide additional services to their corporate clients. The benefits of this development are twofold: It forces the firm to become competent in ESI while providing a new and growing revenue stream.

Understanding what electronic information to maintain, how to maintain it, and for how long is a balancing act involving technology, legal issues, industry standards, and business considerations. A sound document retention policy will have several goals:

- To identify the documents to which the policy applies;
- To reduce the expense of retrieving electronic data stored on obsolete or corrupted back-up systems;
- To reduce search costs in the event that the company is ever required to respond to subpoenas or document requests that might be issued in future lawsuits or investigations;
- To help negate any inference that the company has engaged in spoliation of evidence;
- To identify specific periods of time for document retention;
- To clarify the procedures for retention or destruction and the lines of responsibility in unambiguous terms; and
- To streamline the transfer of potentially responsive ESI from the client to outside counsel or the electronic discovery vendor acting on behalf of outside counsel.

A conflict may arise between document retention policies and the obligation to preserve potential evidence. A policy put into place when litigation is foreseeable may result in allegations of spoliation of evidence. See *Hynix Semiconducter, Inc. v Rambus, Inc.* (ND Cal 2006) 591 F Supp 2d 1038. In *Hynix,* the court considered allegations of evidence spoliation based on the responding party's document destruction on "shred days." The court noted that, although "a legitimate consequence of a document retention policy is that relevant information may be kept out of the hands of adverse parties," a policy "adopted or utilized to justify the destruction of relevant evidence is not a valid

policy." 591 F Supp 2d at 1060. See also *Rambus, Inc. v Infineon Tech. AG* (ED Va 2004) 220 FRD 264, 286 (party guilty of spoliation because "even valid purging programs need to be put on hold when litigation is 'reasonably foreseeable'").

PRACTICE TIP: Counsel may wish to identify in advance a member of the client's information technology (IT) department who will be in a position to verify, if necessary for a court, how the company's ESI is routinely saved, archived, and then purged within a reasonable time period. A company that does not have an IT person in place to testify regarding its normal procedures for handling ESI could be disadvantaged if it becomes necessary to explain why particular ESI is not available.

For further discussion of document retention policies, see Washton, *Document Retention Programs in an Electronic Environment*, 20 CEB Cal Bus L Prac 28 (Winter 2005).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/20A Discovery of Electronically Stored Information/§20A.5 C. Special Problems Concerning E-mail

§20A.5 C. Special Problems Concerning E-mail

Any business contemplating the establishment of a document retention policy should consider the special problem of e-mail communications. Perhaps the most significant potential problem with e-mail is that it is often treated more informally than traditional business letters and memoranda. Corporate managers and employees today are accustomed to using e-mail for informal communication. When e-mail is used in the legal and business environment, however, increased formality in the communication is rarely found unless existing business guidelines require it. For instance, many law firms and corporate legal departments include a header or footer on e-mails with a notice that the communication contains privileged information that should not be read by an unintended recipient. Notwithstanding this warning, it is not unusual for attorneys and executives communicating with attorneys to exchange non-privileged, casual communications using the corporate e-mail system.

In connection with an e-mail retention policy, businesses should consider establishing and implementing e-mail communications guidelines for employees. E-mail guidelines typically emphasize that company computers belong to the company and should be used for business purposes only. See *Sims v Lakeside Sch.* (WD Wash, Sept. 20, 2007, No. C06-1412RSM) 2007 US Dist Lexis 69568. Employees should be informed that they have no expectation of privacy in the use of business electronic communications and that they may be monitored by management in the ordinary course of business. Moreover, e-mails that are deleted by the user are usually not truly and permanently deleted. Most e-mail messages are archived and exist in backup media even if deleted on the local computer or e-mail server where they were created. Compounding this, even "deleted" e-mail messages and other documents that are not archived can normally be fully or partially recovered by a computer forensic technician. Because of these realities, employees should be instructed to take the same care in drafting e-mail communications as they exercised in drafting business letters or memorandums in years past. Employees should also be encouraged to avoid inappropriate humor or tasteless content in e-mail communications, which can seem far harsher and more damaging when reviewed years later, out-of-context, in hard copy. Once e-mail guidelines are established, effective communication programs should be established to implement them and to train employees periodically in the proper use of electronic communications. E-mail guidelines should apply not only to local e-mail accounts and e-mail servers, but also to portable e-mail technologies such as the Blackberry as well as instant messaging and cell phone texting.

The court in *Sims v Lakeside Sch., supra,* addressed the issue of electronic discovery and the expectation of privacy with respect to ESI on an employee's work computer owned and maintained by the employer. In *Sims*, the plaintiff was employed by a public school district. The defendant school district imaged the hard drive of the computer that the plaintiff had used extensively. The plaintiff had sent and received e-mails using the locally installed e-mail program on the work computer and also using a web-based e-mail system. The court held that the employee had no reasonable expectation of privacy in any e-mail messages sent and received via his work computer's local e-mail application—even those exchanged with counsel, which would normally be protected by attorney-client privilege. This finding was based in part on the fact that the school's computer use policy clearly stated that e-mail user accounts remained the property of the school. Although the attorney-client privilege and marital privilege protected e-mails the employee exchanged with counsel and his spouse via web-based e-mail, all other web-based e-mail was subject to discovery. In *Convertino v U.S. Dep't of Justice* (D DC, Dec. 10, 2009, No. 04-0236) 2009 US Dist Lexis 115050, however, the court found reasonable an employee's expectation of privacy in e-mail he sent through his workplace e-mail account because his employer's e-mail policy did not prohibit personal use of the account.

It should be noted that in *Sims*, the focus of the data gathering was the employee's PC, even though some of the employee's e-mail was managed locally and other e-mail was managed over the web via a free webmail portal. The standards change significantly when courts focus on collecting e-mail information directly from the servers of a webmail provider such as Google, America Online (AOL), or Yahoo. In *In re Supoena Duces Tecum to AOL, LLC* (ED Va 2008) 550 F Supp 2d 606, the court was confronted with the task of reviewing a lower court's decision to quash a subpoena for harvesting the opposing party's e-mail, during a defined time frame, directly from the party's e-mail account maintained by AOL. The court upheld the lower court's decision to quash the subpoena, finding that Title II of the

Electronic Communications Privacy Act of 1986 (ECPA) (18 USC §§2701-2712) specifically prohibits a remote web-hosting service from disclosing the contents of a customer's electronic communications except for purposes of a government criminal investigation. The court cited not only the user's expectation of and interest in privacy as grounds for the holding, but further reasoned that the service provider would experience "substantial burden and expense" if it were "required to respond to every civil discovery subpoena issued in a civil lawsuit." 550 F Supp 2d at 611.

PRACTICE TIP: Because most free commercial e-mail hosting services retain e-mails on servers for anywhere from a few days to a few weeks, counsel tasked with requesting e-mail messages hosted "in the cloud" by an online vendor such as Google, AOL, or Yahoo should act quickly.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/20A Discovery of Electronically Stored Information/§20A.6 III. FEDERAL RULES ON ELECTRONIC DISCOVERY

§20A.6 III. FEDERAL RULES ON ELECTRONIC DISCOVERY

Federal Rules of Civil Procedure 16, 26, 33, 34, 37, and 45 and Form 35 address issues related to ESI including, for example, the meaning of the term "document" in relation to discovery of electronically stored information. The rules require "early attention to issues relating to electronic discovery, including the frequently-recurring problems of the preservation of the evidence." Report of the Judicial Conference, Committee on Rules of Practice and Procedure (September 2005). The rules also address procedures for obtaining, reviewing, and producing electronically stored information, and the penalties for noncompliance.

PRACTICE TIP: The Advisory Committee on 2006 Amendments to the Federal Rules of Civil Procedures prepared extensive notes to accompany the amendments. The notes provide helpful guidance in applying the rules to electronic discovery in litigation practice.

© The Regents of the University of California

§20A.7 A. Rule 16: Scheduling Orders

Federal Rule of Civil Procedure 16(b) includes provisions for disclosure or discovery of electronically stored information as a topic that should be discussed before issuance of, and that may be addressed in, the court's pretrial scheduling order. The order may also include any agreements that the parties have reached to minimize the risk of waiver of the attorney-client privilege or work product protection. In conjunction with Fed R Civ P 26(f)(3), the rule is intended to assure that the parties discuss issues related to the discovery of electronically stored information early in the litigation process. See Fed R Civ Proc 16(b), 26(f)(3).

PRACTICE TIP: Counsel should be aware that scheduling orders from many courts, most notably federal district and administrative courts, may arrive via an e-mail notification from the court's electronic filing system.

© The Regents of the University of California

B. Rule 26: General Discovery Provisions; Duty of Disclosure

§20A.8 1. Initial Voluntary Disclosure

Electronically stored information is now expressly included among the categories of information that a party is under a duty to include in its initial disclosures to the other parties in the litigation, without waiting for a discovery request. See Fed R Civ P 26(a)(1)(A)(ii).

In two widely publicized decisions, courts ruled that a party (and its counsel) are legally and morally obligated to produce clearly relevant e-mail information. In *Peskoff v Faber* (D DC 2007) 244 FRD 54, the court required the defendant to conduct a large-scale, comprehensive search of its systems for clearly relevant e-mail messages, which the requesting plaintiff was able to show existed but which were not produced. The court ordered the defendant to conduct the search at its own expense and to provide an affidavit of the person who conducted the search.

PRACTICE TIP: In light of *Peskoff,* it is critical that counsel employ an experienced third party to harvest potentially discoverable ESI from counsel's client. Counsel should confirm that the selected consultant is familiar with and able to employ court-accepted forensic data collection technologies. The qualifications of the person who performs the forensic imaging or analysis of data are important because that person may become an expert witness at trial if questions arise regarding how the data has been handled. Courts may require that professionals who handle data have experience, knowledge, and even forensic certifications in order to make a showing that the data was not mishandled or despoiled.

In *Qualcomm Inc. v Broadcom Corp.* (SD Cal, Jan. 7, 2008, No. 05cv1958-B (BLM)) 2008 US Dist Lexis 911, aff'd in part and rev'd in part on other grounds (Fed Cir 2008) 548 F3d 1004, a patent infringement suit that attracted mainstream media attention, Magistrate Judge Barbara Major of the U.S. District Court for the Southern District of California found that the plaintiff Qualcomm "intentionally withheld tens of thousands of decisive documents from its opponent in an effort to win this case and gain a strategic business advantage." 2008 US Dist Lexis 911 at *32. The magistrate found that Qualcomm could not have succeeded in withholding 46,000 e-mails and other requested documents "without some type of assistance or deliberate ignorance from its retained attorneys." 2008 US Dist Lexis 911 at *32.

NOTE: The court found that Qualcomm's attorneys had removed e-mails from files before preparing employees for testimony and concluded that "Qualcomm's counsel participated in an organized program of litigation misconduct and concealment throughout discovery, trial and post-trial before new counsel took over lead role in the case." *Qualcomm Inc. v Broadcom Corp.* (SD Cal 2007) 539 F Supp 2d 1214, 1234, aff'd in part and rev'd in part on other grounds (Fed Cir 2008) 548 F3d 1004. Such a judicial response to a party that fails to produce ESI or that is suspected of affirmative misconduct by attempting to hide, destroy, or otherwise not produce such evidence may become more common in the future.

Despite the benefit of a waiver of the attorney-client privilege with respect to their efforts to defend themselves, the six attorneys and Qualcomm were ultimately sanctioned more than $8.5 million in attorney fees and costs for their "monumental and intentional discovery violation." 2008 US Dist Lexis 911 at *63. Both Qualcomm and the six attorneys were ordered to participate in a Case Review and Enforcement of Discovery Obligations (CREDO) program and to submit progress reports to the court. The attorneys were referred to the State Bar for an investigation of possible ethical violations. 2008 US Dist Lexis 911 at *64.

The *Qualcomm* case illustrates the high stakes at play with respect to modern electronic discovery. It further illustrates that judicial inquiries pertaining to electronic discovery frequently center around ethical issues and malpractice claims. The modern litigator can never be too careful when conducting electronic discovery.

© The Regents of the University of California

§20A.9 2. "Clawback" of Privileged Material

Federal Rule of Civil Procedure 26(b)(5) includes a "clawback" procedure for asserting attorney-client privilege or work product protection *after* production, under which the recipient of the privileged matter is required to promptly return, sequester, or destroy the specified information (and any copies that it has). The recipient may not use or disclose the information until the privilege claim is resolved. For further discussion of the Rule 26(b)(5) procedures for retrieval of privileged information, see §20A.44. Similarly, Rule 34(a) provides that where excessive quantities of ESI are produced, the requesting party may "sneak a peek" by sampling the ESI. If relevant information is found, then the ESI must be produced. If nothing relevant is found, the court may issue a protective order relieving the producing party from continuing with production of irrelevant data. Privileged information is ignored and not deemed produced. See California Civil Discovery Practice, chaps 4 and 8 (4th ed Cal CEB 2006). See also the discussion of Fed R Evid 502 in §20A.44A.

PRACTICE TIP: A party that inadvertently produces privileged ESI to the requesting party should notify the requesting party in writing immediately on learning that privileged information has or may have been inadvertently produced. Courts have held that a failure to promptly notify the party in possession of privileged material may result in a waiver of privilege. See *Brookdale Univ. Hosp. & Med. Ctr., Inc. v Health Ins. Plan of Greater N.Y.* (ED NY, Feb. 13, 2009, No. 07 CV 1471) 2009 US Dist Lexis 11537.

© The Regents of the University of California

§20A.10 3. Meet-and-Confer Requirements

Parties are required to discuss any issues relating to disclosure or discovery of electronically stored information as part of the meet-and-confer process, including the form in which ESI is to be produced. Fed R Civ P 26(f)(3)(C). As a practical matter, this means that counsel must have a working knowledge of computer technology so that counsel can intelligently discuss the data infrastructures of both the client and the opponent and negotiate an effective ESI discovery plan. See §20A.29.

The parties are also required to discuss issues relating to claims of attorney-client privilege and work product protection, including claims made after production. See Fed R Civ P 26(f)(3)(D).

© The Regents of the University of California

§20A.11 4. Safe Harbor if ESI Not Reasonably Accessible

Federal Rule of Civil Procedure 26(b)(2)(B) limits the potential scope of electronic discovery by providing a safe harbor for the responding party asked to produce electronically stored information "from sources that the party identifies as not reasonably accessible because of undue burden or cost." Under Fed R Civ P 26(b)(2)(B), a party asked to produce ESI from sources "not reasonably accessible" has the burden of describing why the requested ESI is not reasonably accessible. Then, if the responding party meets its burden, the burden shifts to the requesting party to demonstrate "good cause" why the evidence should be produced.

If the requesting party shows good cause, considering the limitations of Fed R Civ P 26(b)(2)(C), the court may order the responding party to produce discovery from those sources. Factors that the court may consider in determining whether good cause exists include the following (Advisory Committee Notes, 2006 Amendment to Rule 26):

- The specificity of the discovery request;
- The quantity of information available from other and more easily accessed sources;
- The failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources;
- The likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources;
- Predictions as to the importance and usefulness of the further information;
- The importance of the issues at stake in the litigation; and
- The parties' resources.

Whether data that can be used only by superseded systems, *i.e.,* legacy data, must be produced in usable form depends on whether its production would be unduly burdensome. See Fed R Civ P 26(b)(2)(B). In general, the Advisory Committee notes that litigation parties should consider "the balance between the competing needs to preserve relevant evidence and to continue routine operations critical to ongoing activities. Complete or broad cessation of a party's routine computer operations could paralyze the party's activities." Advisory Committee Notes, 2006 Amendment to Rule 26(f). The courts have apparently not yet clarified whether the requesting party or the producing party should pay for special hardware (usually long outdated drives or tape players) if required to view or examine legacy data.

© The Regents of the University of California

§20A.12 C. Rule 33: Interrogatory Responses

Federal Rule of Civil Procedure 33(d) adds electronically stored information to the category of information that may be included in responses to interrogatories if the information can be accessed by the requesting party as "readily" as by the party served with the interrogatory.

© The Regents of the University of California

D. Rule 34: Production of Documents and Things

§20A.13 1. Rule 34(a): Inspection, Copying, Testing, and Sampling

The federal rules recognize electronically stored information as a category subject to discovery that is distinct from "documents" and "things." Federal Rule of Civil Procedure 34(a)(1)(A) expressly permits parties to "inspect, copy, test, or sample… electronically stored information." However, the access that accompanies a requesting party's right to inspect, copy, test, and sample the responding party's electronically stored information "is not meant to create a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances." Advisory Committee Notes, 2006 Amendment to Rule 34. Federal Rule of Civil Procedure 34 allows testing or sampling of ESI to enable the requesting party to determine which parts of voluminous electronically stored information might contain relevant information and be worth searching in terms of time and expense. See Fed R Civ P 34(a); California Civil Discovery Practice, chaps 4, 8 (4th ed Cal CEB 2006). For further discussion of a party's right to an on-site inspection of its opponent's systems, see §20A.38. See also the discussion of Fed R Evid 502 in §20A.44A.

© The Regents of the University of California

§20A.14 2. Rule 34(b): Specifying Format for Production

Under the federal rules, a requesting party may specify the form or forms in which the electronically stored information is to be produced. Fed R Civ Proc 34(b)(1)(C). If the requesting party does not specify a particular form, data must be produced in the form "in which it is ordinarily maintained" or in "reasonably usable" form. Fed R Civ Proc 34(b)(2)(E)(ii). The form in which a file is ordinarily maintained is known as its "native" format. See §20A.40.

NOTE: Native files usually contain invisible metadata, and counsel should be aware of the information contained within the metadata that will "travel" with the native file to opposing counsel.

The file should not be converted to a different format that might hamper the requesting party's purposes. "If the responding party ordinarily maintains the information it is producing in a way that makes it searchable by electronic means, the information should not be produced in a form that removes or significantly degrades this feature." Advisory Committee Notes, 2006 Amendment to Rule 34. Similarly, electronic documents should not be changed to a format that eliminates or alters metadata. See §20A.36. The revised rule is intended to provide an ESI analogue to the previous language that prevents massive "dumps" of disorganized documents by requiring production of documents either as they are ordinarily maintained or else organized and labeled to correspond with the categories in the request for production.

© The Regents of the University of California

§20A.15 E. Rule 37: Safe Harbor for Routine Deletion

Federal Rule of Civil Procedure 37(e) provides a safe harbor from sanctions for a party that cannot produce data because it was destroyed in good faith due to routine operation of its information systems. See §20A.4. For example, to prevent computer operating systems from being overwhelmed with redundant files, starting a computer will often remove or significantly alter cached files and other temporary files to make room for new files. When litigation is pending or underway, a custodian of discoverable electronic information may be obligated to interfere with routine system operations that might otherwise delete data subject to a preservation obligation.

This safe harbor does not protect a party who allows routine operations to destroy information subject to a litigation hold. Advisory Committee Notes, 2006 Amendment to Rule 37. For discussion of litigation holds, see §§20A.25-20A.26.

© The Regents of the University of California

§20A.16 F. Rule 45: Response to Subpoenas

Revisions to Fed R Civ Proc 45, which governs subpoenas, conform to the recent amendments to Fed R Civ P 26 and 34. Among the changes in the rule pertaining to e-discovery are the following:

- Rule 45(a)(1)(C): "[E]lectronically stored information," as defined in Rule 34(a), is among discoverable material that may be subpoenaed.
- Rule 45(d)(1)(B): Unless otherwise specified, electronically stored information must be produced in the form in which it is ordinarily maintained, or in "reasonably usable" form.
- Rule 45(d)(1)(D): Information not readily accessible because of "undue burden or cost" need not be produced.

© The Regents of the University of California

IV. CALIFORNIA LAW

§20A.17 A. Rules of Court

Effective August 14, 2009, the California Judicial Council amended the Rules of Court to add discovery of electronically stored information to the topics on which parties must meet and confer before their initial case management conference. See Cal Rules of Ct 3.724(8). Issues mandated for discussion include the scope of ESI discovery, preservation of ESI, the form of production, and the allocation of costs.

The rule also requires parties to discuss the means of preserving and asserting claims of privilege, and whether such claims should be permitted postproduction. Cal Rules of Ct 3.724(8)(E). See also the discussion of privilege in §20A.44.

© The Regents of the University of California

§20A.18 B. Electronic Discovery Act

California's Electronic Discovery Act (Stats 2009, ch 5), effective June 29, 2009, amended the Civil Discovery Act (CCP §§2016.010-2036.050) to define electronically stored information (see CCP §2016.020(d)-(e)) and make it fully amenable to inspection, duplication, testing, or sampling by any party to a legal action (see CCP §2031.010(a)). The Act is modeled after, and largely identical to, the Federal Rules of Civil Procedure relating to discovery of ESI, discussed in §§20A.6-20A.16. Like the ESI-related amendments to the Federal Rules of Civil Procedure 3 years before, the Act modernizes longstanding discovery rules that were crafted for paper-based and testimonial discovery. The amended rules are intended to meet the needs of litigators who must exchange and review evidence that is generated and stored digitally and may never assume a paper-based format (less than 3 percent of computer-generated documents are ever printed to paper).

© The Regents of the University of California

§20A.18A 1. ESI From Sources Not Reasonably Accessible

One of the Electronic Discovery Act's few variations from the federal rules concerns a demand for production of electronically stored information "from a source that is not reasonably accessible because of undue burden or expense." CCP §§1985.8(d)-(e), 2031.060(c)-(e), 2031.310(d)-(e). Under Fed R Civ P 26(b)(2)(B) (discussed in §20A.11), the responding party has the initial burden of describing in writing which ESI it is unwilling to produce and how and why it is not reasonably accessible. If the responding party meets its burden, the burden shifts to the *requesting* party to file a motion to compel production based on "good cause" and a showing that the evidence should be produced nonetheless given its heavy probative value. In contrast, the California rule requires the *responding* party to file a motion for a protective order and demonstrate that the requested information is truly from a source that is not reasonably accessible because of undue burden or expense. Even if the responding party meets its burden, however, the court may deny a protective order and compel production for "good cause." CCP §§1985.8(f), 2031.060(e), 2031.310(f). The "good cause" standard has yet to be developed by the California courts.

NOTE: A party that objects to discovery of ESI on the grounds that it is from a source not reasonably accessible and declines to search the source absent an agreement with the demanding party or a court order must identify in its written response to the demand the types or categories of sources it asserts are not reasonably accessible. CCP §2031.210(d). Meeting this requirement preserves any objections the responding party may have regarding the electronically stored information.

The court that orders production of information demonstrated to be from a source that is not reasonably accessible may allocate the expense of producing the information. CCP §2031.060(e).

© The Regents of the University of California

§20A.18B 2. Safe Harbor for Lost Information

The California "safe harbor" provision for lost information, like the federal provision discussed in §20A.15, restricts a court's ability to sanction a party if it cannot produce ESI because that ESI was "lost" as a result of the good faith operation of an electronic information system. California extends its rule further to restrict a court from sanctioning a litigant whose ESI is not only "lost" but may be unavailable because it was "damaged, altered or overwritten" by an electronic information system. CCP §§2031.060(i), 2031.300(d)(1), 2031.320(d)(1).

© The Regents of the University of California

§20A.18C 3. Disclosure of Privileged Information

Like the federal rules (see §20A.9), the California Electronic Discovery Act includes a "clawback" provision to enable a party who inadvertently produces privileged information to cure the oversight and attempt to preserve attorney-client confidences. See CCP §§1985.8(i), 2031.285. Under the California rule, the party that inadvertently produced the privileged ESI may seek return of the information by notifying the opposing side of the inadvertent production and describing the inadvertently produced information with particularity. CCP §2031.285(a). Pending resolution of the claim, the receiving party must "immediately sequester the information and either return the specified information and any copies that may exist or present the information to the court conditionally under seal for a determination of the claim." CCP §2031.285(b). The receiving party is precluded from using or disclosing the information at issue until the privilege claim is resolved. If the receiving party has disclosed the information before being notified of a claim of privilege, the receiving party must promptly take reasonable steps to retrieve the information. CCP §2031.285(c)(2). The receiving party may, within 30 days of being placed on notice that it received privileged information, file a motion disputing the producing party's claim. CCP §2031.285(d)(1). Until the court rules on the privilege claim, the receiving party must preserve and keep confidential the information and may not use it in any manner. CCP §2031.285(d)(2).

© The Regents of the University of California

§20A.18D 4. Form of Production

The demanding party is required to specify "the form or forms" in which each type of ESI may be produced. CCP §§1985.8(b), 2031.030(a)(2). The California rules also provide that unless otherwise specified in the demand, information may be produced in the form "in which it is ordinarily maintained or in a form that is reasonably usable." CCP §§1985.8(c)(1), 2031.280(d)(1). Electronically stored information need not be produced in more than one form. CCP §§1985.8(c)(2), 2031.280(d)(2).

© The Regents of the University of California

§20A.18E 5. Court-Imposed Limits on Production

The federal and California rules differ with respect to a court's authority to limit production. In contrast to the federal rules, a California court may impose limits on the scope of production sua sponte if the court finds that the ESI may be produced from a less burdensome source, that the data requested appears to be unreasonably duplicative, or that the burden of production outweighs the benefit of the data as evidence. CCP §§1985.8(h), 2031.310(g).

© The Regents of the University of California

V. ADVANCE PREPARATION FOR DISCOVERY OF ESI

§20A.19 A. ESI Survey and Retention Policy

Litigation in federal and California courts nearly always involves electronically stored information as potential evidence, and both plaintiff and defendant are likely to be subject to requests for production of ESI. Before an investigation or litigation looms, companies should survey their ESI and ESI retention policies with the goal of determining how best to locate and organize data in response to any potential future discovery request. Companies should assure themselves that they are not following inadequate document retention policies.

PRACTICE TIP: Companies should consider installing management appliances for electronically stored information such as Clearwell Systems or ActiveVault that allow them to automate retention policies and filter and control data as it is previewed before delivery to outside counsel or the requesting party. See §20A.4.

Mishandling of ESI may result in sanctions for spoliation of evidence if it appears that data that would be of interest to a requesting party (and the court) has been purposefully or negligently destroyed. See *Zubulake v UBS Warburg* LLC (SD NY 2003) 220 FRD 212.

© The Regents of the University of California

§20A.20 B. Identifying Key Personnel

Counsel should consider forming a cross-disciplinary team to help prepare for and implement electronic discovery if and when the need arises. The team should have members who are knowledgeable about the client's information technology (IT), IT applications, structure, and records systems, as well as the facts of any anticipated or threatened litigation. The client should designate an individual, not necessarily a lawyer, who is knowledgeable about the company's electronic systems and capabilities and who would be able to confer intelligently with interested parties before or during discovery.

The team should consider the scope of data collection, and address the following questions:

- Should data be collected from across the entire organization or only from certain departments or individuals?
- Is data presently online and immediately accessible ("live" data)?
- Are archived forms of data such as backup tapes or optical disks involved?
- Which backups, servers, desktops, and remote devices (such as PDAs, cell phones, laptops, fax machines, voice-mail storage, or home computers) might be involved?
- Can data be gathered across the network from a central location?
- Is it possible to simply restore data captured to archival media such as backup tapes and avoid the need to harvest data from active drive sources?
- Will data need to be copied at local workstations?

The team should also decide how to make a record of the data collection process and evaluate the likelihood of chain-of-custody issues.

© The Regents of the University of California

VI. RETENTION OF ESI WHEN LITIGATION IS PENDING

§20A.21 A. Notice of Litigation

The pendency of litigation or the possibility of future litigation may trigger the duty to preserve data. A duty to preserve data arises when a party "has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation." *Zubulake v UBS Warburg LLC* (SD NY 2003) 220 FRD 212, 216. A party can be put on notice to preserve data long before litigation is initiated. *Goodman v Praxair Servs., Inc.* (D Md 2009) 632 F Supp 2d 494, citing *Silvestri v General Motors Corp.* (4th Cir 2001) 271 F3d 583, 591 ("duty to preserve material evidence… also extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation"). Further, counsel should inquire about any informal communications that could have indicated the possibility of future litigation. "Pre-filing communications between the litigants can… provide constructive notice that litigation is likely." 271 F3d at 511.

Events that may be considered indicators of potential litigation include the following:

- The receipt or sending of a demand letter.
- The receipt of oral notification that a complaint might be filed. See, *e.g., Capellupo v FMC Corp.* (D Minn 1989) 126 FRD 545, 551 (employee told company EEO manager that she was contemplating a class-action gender discrimination suit and EEO officer relayed this to others at company headquarters).
- The receipt of a complaint in a case. See, *e.g., Clark Constr. Group v City of Memphis* (WD Tenn 2005) 229 FRD 131, 137 (on date complaint was filed, at the latest, city knew it must safeguard documents).
- The receipt of a court order. See *E*Trade Secs. LLC v Deutsche Bank AG* (D Minn 2005) 230 FRD 582, 589 (defendants knew about potential for litigation involving certain transactions when they received bankruptcy order).
- The receipt of a subpoena.
- The receipt of notice of a governmental investigation.
- The awareness of an accident or incident that may give rise to litigation. See, *e.g., Stevenson v Union Pac. R.R.* (8th Cir 2004) 354 F3d 739, 747 (railroad had been involved in numerous grade crossing collisions and knew taped conversations between train crew and dispatch would be relevant to any potential litigation about accident); *Broccoli v Echostar Communications Corp*. (D Md 2005) 229 FRD 506, 510 (employee's oral and e-mailed complaints of harassing behavior gave employer actual notice to preserve all documents, including e-mail and personnel files, relating to the complaints).
- The awareness of an enforcement proceeding or investigation that may target the party. See, *e.g., Alliance to End Repression v Rochford* (ND Ill 1976) 75 FRD 428, 440 (defendants had duty to preserve records when paid informants told defendants that plaintiffs seemed ready to proceed with lawsuit).

Preservation of data when litigation is anticipated is known as a "litigation hold." See §20A.25.

NOTE: In a few jurisdictions, such as Colorado, only filing a complaint and the existence of a lawsuit will trigger preservation duties. See *Cache La Poudre Feeds, LLC v Land O' Lakes, Inc*. (D Colo 2007) 244 FRD 614, 623 (defendants' duty to preserve was triggered by filing of complaint and not by earlier demand letters that were equivocal and "less than adamant").

© The Regents of the University of California

§20A.22 B. Duty to Preserve Evidence

It is important for counsel to advise the client to take reasonable measures to preserve evidence when the client's duty to do so arises. As discussed in §20A.21, an obligation to preserve evidence generally arises when the party has notice that the evidence is potentially relevant or reasonably likely to be requested during discovery. The duty to preserve evidence is triggered when that party "should have known that the evidence may be relevant to future litigation." *John B. v Goetz* (6th Cir 2008) 531 F3d 448, 459.

Further, evidence must be preserved before the filing of a complaint. *Goodman v Praxair Servs., Inc.* (D Md 2009) 632 F Supp 2d 494, citing *Silvestri v General Motors Corp.* (4th Cir 2001) 271 F3d 583, 591 ("duty to preserve material evidence… extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation").

In *Cedars-Sinai Med. Ctr. v Superior Court* (1998) 18 C4th 1, 12, 74 CR2d 248, the California Supreme Court stated:

> As a practical matter, modern civil discovery statutes encourage a lawyer to marshal and take charge of the client's evidence, most often at an early stage of the litigation. In doing so, a lawyer customarily instructs the client to preserve and maintain any potentially relevant evidence, not only because it is right for the client to do so but because the lawyer recognizes that, even if the evidence is unfavorable, the negative inferences that would flow from its intentional destruction are likely to harm the client as much as or more than the evidence itself.

Because the failure to preserve evidence may have extraordinary consequences in terms of sanctions, most attorneys consider it best to counsel their clients to preserve electronic data whenever an event has occurred that may trigger a duty to preserve, even before receiving formal notification that data may be relevant to a dispute.

In the most general terms, a party must not destroy "unique, relevant evidence that might be useful to an adversary." *Zubulake v UBS Warburg LLC* (SD NY 2003) 220 FRD 212, 217. Spoliation of evidence is "the destruction or significant alteration of evidence, or the failure to properly preserve property for another's use as evidence pending or reasonably foreseeable litigation," and may result in sanctions against the offending party. 220 FRD at 216.

The manner in which electronic evidence is discussed in §20A.27. Sanctions for destruction of evidence are discussed in §20A.28.

© The Regents of the University of California

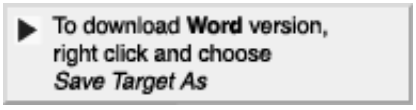
C. Legal Hold Letter to Client

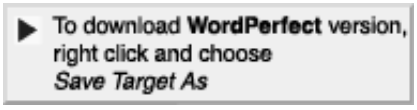
§20A.23 1. Legal Holds

An attorney who believes his or her client has the responsibility to preserve evidence should consider sending (or ensuring that the client sends) a "legal hold" letter to all persons who have the potential to destroy information that may be relevant to the subject of the case. See §20A.24 for a suggested form. Generally, counsel should make sure that the legal hold letter is sent to the IT department so that IT can stop implementing any existing automatic document or information destruction policy.

© The Regents of the University of California

§20A.24 2. Form: Legal Hold Letter to Client





_ _[*date*]_ _
_ _[*name*]_ _
_ _[*address*]_ _
Dear _ _[*name*]_ _**:**

_ _[*Name of client*]_ _ **has been named in a lawsuit relating to** _ _[*supply information about the matter*]_ _**. You may have records or information relating to this lawsuit. This letter contains important directions about preserving relevant records and information. Please make sure you understand these directions. These directions supersede all other records retention policies—even records that would ordinarily be destroyed as part of** _ _[*name of client*]_ _**'s routine records management program must be preserved. Please contact me if you have any questions regarding these directions.**

Please retain all records that contain any information relating to this matter. These records must be retained and maintained until you are informed by the Legal Department that the matter has been concluded and the records no longer need to be retained.

"Records" means anything that stores information:

· In any medium: paper, electronic, and video- and audiotape, including e-mails, voice-mail, text messages, and any other electronic files;

· In any form: handwritten or typed, draft or final, desk or electronic calendars;

· Created at any time, including documents you created in the past, as well as any documents you may create from this date forward;

· Wherever maintained: whether on your computer, in your office, in departmental files, in a home office, on a home computer, in your car, or elsewhere.

You must retain any and all records that contain any information that has any connection whatsoever to this matter or to any of the issues summarized in the paragraph below. Even if the relevant information is only a small portion of a particular record—for example, a single bullet point in a comprehensive business or strategic plan—you must retain the entire record. If you are uncertain whether a document relates to this matter, retain it, and then check with me to determine whether to continue to retain it.

This matter involves _ _[*supply information about the matter*]_ _**. The Plaintiff(s),** _ _[*name(s)*]_ _**, allege(s) that** _ _[*set forth the allegations*]_ _**. You must retain any records that relate to these issues, including (among others) the following records:** _ _[*identify any specific records*]_ _**.**

If the specified records exist in paper form, you must keep them, without alteration, organized in the way you would normally keep them for business purposes. For example, if you normally keep them in file folders, continue to do so. Unless your home office is your principal office, the records should be kept at a company location within the control of you or your department. Electronic records should generally be kept in electronic form. To the extent that any such records involve data that continually changes, you may satisfy the retention requirements by printing and retaining a monthly summary. If electronic files were created but not retained, please contact me and we will determine how best to recover these documents, including e-mails sent and received.

If you believe this letter should be sent to anyone else, please advise me. If you are aware of other

individuals not on the distribution list who might have documents relating to this matter, including outside contractors and vendors, please let me know and I will send them a copy of this letter. Please do not send the letter to other company employees yourself; I want to keep a record of all individuals to whom the letter is sent.

Please notify me promptly in the event you are leaving _ _[*name of client*]_ _ or changing jobs within _ _[*name of client*]_ _. I will make arrangements to appropriately preserve the documents you are maintaining in accordance with this notice.

I have attached some important reminders about document creation and inquiries from third parties regarding this matter.

Thank you for your cooperation in this important matter. If you have any questions, please contact me at _ __ _[*phone number or e-mail address*]_ _.

Date: _ _ _ _ _ _ _ _[*Name of firm*]_ _

By: __[*Signature*]__
_ _[*Typed name*]_ _
Attorney for _ _[*name*]_ _

Comment: For an example of a legal hold imposed by court order, see *Westcoat v Bayer CropScience LP* (ED Mo, Nov. 1, 2006, No. 4:06-cv-01529-ERW) 2006 US Dist Lexis 79756.

© The Regents of the University of California

D. Litigation Hold Letter to Opponent

§20A.25 1. Litigation Holds

It is usually advisable for counsel to send the responding party a preservation-of-evidence letter (also known as a "spoliation letter" or "litigation hold letter") at an early stage of the litigation (and perhaps even before litigation commences). See *Pension Comm. of Univ. of Montreal Pension Plan v Banc of Am. Sec.* (SD NY, Jan. 15, 2010, No. 05 CIV 9016) 2010 US Dist Lexis 1839, *10 (after *Zubulake v UBS Warburg LLC* (SD NY 2003) 220 FRD 422, "failure to issue a written litigation hold constitutes gross negligence"). For a sample letter, see §20A.26. Ideally, the letter should be as specific and detailed as possible regarding the issues in the litigation, the types of electronic materials that the party believes should be preserved, and the manner in which they should be preserved. See *In re FirstEnergy Corp. Sec. Litig.* (ND Ohio 2004) 229 FRD 541, 543, in which plaintiffs detailed the precise steps and methods by which defendants were to preserve specified electronic evidence. The general scope of a litigation hold was described in one of the *Zubulake* decisions as follows (*Zubulake v UBS Warburg LLC* (SD NY 2003) 220 FRD 212, 218):

> The scope of a party's preservation obligation can be described as follows: Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents. As a general rule, that litigation hold does not apply to inaccessible backup tapes (e.g., those typically maintained solely for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth in the company's policy. On the other hand, if backup tapes are accessible (i.e., actively used for information retrieval), then such tapes would likely be subject to the litigation hold.

Preservation letters, particularly if sent before litigation formally commences, help protect the sending party against the recipient's destruction of evidence and later attempts to claim that it was unaware that the evidence was relevant to the litigation.

In a later *Zubulake* decision, *Zubulake v. UBS Warburg LLC* (SD NY 2004) 229 FRD 422, the court emphasized the duty of counsel for the recipient in implementing the litigation hold. Counsel should oversee compliance with the litigation hold and monitor the recipient's efforts to retain and produce relevant documents. Communication with the client is important to assure that all relevant information is discovered, that relevant information is retained on a continuing basis, and that relevant non-privileged material is produced to the opposing party. 229 FRD at 432.

© The Regents of the University of California

§20A.26 2. Form: Litigation Hold Letter to Opponent

▶ To download **Word** version, right click and choose *Save Target As*

▶ To download **WordPerfect** version, right click and choose *Save Target As*

_ _[*date*]_ _

_ _[name]_ _
_ _[address]_ _

Re: _ _[*description of matter*]_ _

Dear _ _[*name*]_ _:

The purpose of this letter is to notify you and your client, _ _[*name of client*]_ _, not to destroy, conceal, or alter any information stored in electronic form or generated by your client's computer systems or electronic devices. This information may be relevant to the above matter and be unavailable from any other source. As you may know, such electronic information can easily be inadvertently destroyed, and the failure to take reasonable measures to preserve it pending the completion of discovery can result in sanctions being imposed against you or your client. See, *e.g., Cedars-Sinai Med. Ctr. v Superior Court* (1998) 18 C4th 1, 74 CR2d 248; *Zubulake v UBS Warburg LLC* (SD NY 2003) 220 FRD 212, 216.

In order to comply with the discovery requests that we will make in this matter, your client will need to provide electronic evidence in its native format. Your client will also need to provide electronic documents, along with the metadata or information about data that is contained in those electronic documents. Even when a paper copy of a document or file exists, we will also seek the documents or files in their electronic format so that we also receive the information in the metadata. Our discovery requests will include certain data on your client's hard drives, floppy disks, and backup files, and will include data not usually available to the ordinary computer user, such as deleted files and file fragments.

Thus, the electronic data and the storage devices in which they are kept that you and your client are obligated to maintain and preserve during the pendency of discovery in this case include all of the following data and devices:

1. Electronic files, including deleted files and file fragments, stored in machine-readable format on magnetic, optical, or other storage media, including hard drives or floppy disks in your client's desktop computers, laptop computers, home personal computers, and the backup media used for each;

2. E-mail, both sent and received, internally or externally;

3. Telephone files and logs such as voice-mail and universal mobile telecommunications system (UMTS) data;

4. Word processing files, including drafts and revisions;

5. Spreadsheets, including drafts and revisions;

6. Databases;

7. Electronic files in portable storage devices, such as floppy disks, compact disks, digital video disks, ZIP drives, thumb drives, or pen drives;

8. Computer-aided design files;

9. Presentation data or slide shows, such as PowerPoint;

10. Graphs, charts, and other data produced by project management software;

11. Data generated by calendaring, task management, and personal information management software, such as Microsoft Outlook;

12. Data created with the use of personal data assistants, such as PalmPilot;

13. Data created with the use of document management software;

14. Data created with the use of paper and electronic mail logging and routing software;

15. Internet and web-browser-generated history files, caches, and "cookies" files generated at the workstation of each employee in your client's employ and on any and all backup storage media;

16. Logs of network use by your client's employees, whether kept in paper or electronic format;

17. Copies of your client's backup tapes and the software necessary to reconstruct the data on those tapes on each and every personal computer or workstation and network server in your client's control and custody;

18. Electronic information in copiers, fax machines, and printers.

Thank you for your attention to this letter.

Date: _ _ _ _ _ _ _ _[*Name of firm*]_ _

By: __[*Signature*]__
_ _[*Typed name*]_ _
Attorney for _ _[*name*]_ _

Comment: For an example of a legal or litigation hold imposed by court order, see *Westcoat v Bayer CropScience LP* (ED Mo, Nov. 1, 2006, No. 4:06-cv-01529-ERW) 2006 US Dist Lexis 79756.

© The Regents of the University of California

§20A.27 E. Manner of Preservation

Courts continue to consider whether, once the duty to preserve electronically stored information is triggered, the information must be preserved in the same format in which it was created or whether a party may convert it to an inaccessible format, which makes later discovery of the information more difficult and expensive. Compare *Treppel v Biovail Corp.* (SD NY 2006) 233 FRD 363, 372 n4 (conversion of electronic evidence to less accessible form is violation of preservation obligation), with *Quinby v WestLB AG* (SD NY, Dec. 15, 2005, No. 04-CIV-7406) 2005 US Dist Lexis 35583 at *27 n10 (declining to sanction defendant for converting electronic evidence to inaccessible format, even though defendant should have anticipated litigation).

Both federal and California rules permit the requesting party to specify the format of production. Fed R Civ P 34(b)(1)(C); CCP §1985.8(b). If a demand for production does not specify a form or forms for producing a type of electronically stored information, the responding party must produce the information in the form "in which it is ordinarily maintained or in a form that is reasonably usable." CCP §2031.280(d). See §20A.18D.

For further discussion of this issue, see §§20A.39-20A.43.

© The Regents of the University of California

§20A.28 F. Sanctions for Failure to Preserve

In both federal and state courts, if a party is under a duty to preserve electronic evidence and fails to do so, that party may face sanctions for spoliation of the electronic evidence. *In re Napster, Inc. Copyright Litig.* (ND Cal 2006) 462 F Supp 2d 1060. Those sanctions may include:

- An inference that the destroyed evidence would have been unfavorable to the party responsible for its destruction (commonly known as the "adverse inference" sanction);
- Exclusion of witness testimony proffered by the party responsible for destroying the evidence;
- Dismissal of the claim or claims of the party responsible for destroying the evidence;
- Monetary sanctions; and
- Disciplinary sanctions (through a referral to the State Bar for investigation, possibly followed by discipline up to and including disbarment).

In federal court, sanctions for willfully thwarting discovery may include entry of a default judgment against the offending party. Fed R Civ Proc 37(b)(2)(A)(vi). See, *e.g., Coleman (Parent) Holdings, Inc. v Morgan Stanley & Co.* (Fla Cir Ct, Mar. 1, 2005, No. 502003CA005045XXOCAL) 2005 WL 679071, discussed in §20A.2. In *PML N. Am. v Hartford Underwriters Ins. Co.* (ED Mich, Dec. 20, 2006, No. 05-CV-70404-DT) 2006 US Dist Lexis 94456, the court held that considering the responding party's "evasiveness, obfuscation and tampering with important evidence," a default judgment was an appropriate sanction. In addition to the reformatting of a hard drive on the date of the complaint, the court noted other abuses (2005 US Dist Lexis 94456 at *15):

> The inoperable external hard drive is perhaps most damning. Innocent neglect does not cause stripped screws, bent sheet metal, missing parts and other evidence of deliberate tampering and destruction. The court does not accept [the responding party's] clumsy attempt to appear ignorant and therefore less culpable. Even if the court did adopt a more benign view…there is a point beyond which bumbling and blindness to a party's discovery obligations sufficiently resemble the sort of willful, intentional and malicious conduct that calls for the heavy sanction of judgment by default.

For a discussion of whether dismissal is appropriate when evidence has been destroyed, see *Miller v Holzmann* (D DC, Jan 17, 2007, No. 95-01231) 2007 US Dist Lexis 2987 (case may not be dismissed for loss of evidence until lesser alternatives explored and found futile or ineffective to cure the prejudice caused defendants and the court, although other sanctions appropriate). See also *E*Trade Secs. LLC v Deutsche Bank AG* (D Minn 2005) 230 FRD 582 (although default judgment not granted, sanctions against responding party that "wiped clean" its hard drives included damages and adverse inference instruction).

© The Regents of the University of California

VII. DISCOVERY OF ESI

A. Identifying Data for Discovery

§20A.29 1. Need to Understand ESI Infrastructure

Whether the client is a plaintiff or defendant in a lawsuit, it is essential that counsel understand the type of computer systems, networks, file servers, e-mail servers, mobile devices, and other technological infrastructures that the client maintains. In the event of litigation, counsel will require corresponding knowledge of the opponent's technology infrastructure. Counsel should interview the client's IT staff as well as data custodians and, in the event of litigation, counsel should depose the opposing party's IT staff and data custodians to gain this information. Federal and California rules permit an interview of the person "most knowledgeable" about the data infrastructure. See Fed R Civ P 26(b)(1); CCP §2017.010; California Civil Discovery Practice §4.15 (4th ed Cal CEB 2006). See also §20A.30.

PRACTICE TIP: An attorney who is knowledgeable about his or her own client's electronic infrastructure or technology in general will be better prepared to ask pertinent questions of an adversary's data custodian.

Gathering the following information is critical to forming a plan for discovery of electronic information:

- Names of the custodians of information that may be useful in litigation;
- Nature of reports routinely generated by the custodians;
- Location of information—desktops, laptops, PDAs, cell phones, external storage devices such as flash drives;
- Make, model, and hard drive size of desktops, laptops, and servers containing potentially relevant ESI;
- Type of operating system running the machines designated for a data collection;
- Names and contact information of IT personnel who may facilitate access to data that is potentially relevant to the litigation;
- Applications commonly used to create information;
- Whether use of social networking sites such as Facebook and Twitter is allowed, and if so, whether custodians post business-related information to such sites;
- Purpose for which data is created;
- Method and frequency of data backups as well as the location (if any) of redundant data systems and mirror drives;
- How data is used;
- Means of accessing data; and
- Passwords and any other impediments to gaining access to data.

Up-to-date maps of a party's computer networks can be useful to narrow the search for relevant information.

NOTE: Courts have held that data stored temporarily (often for a few hours or less) as RAM is considered ESI and is as discoverable as more permanently stored electronic files. See *Columbia Pictures, Inc. v Bunnell* (CD Cal 2007) 245 FRD 443.

© The Regents of the University of California

§20A.30 2. Drafting a Request for Production

As discussed in §20A.29, an astute litigator will make efforts to understand the responding party's data topography before drafting a request for production of ESI. A well-drafted request for production will designate the location of electronic files sought, the custodians or users of the data (such as e-mail boxes), and the format of production (native files or images of the data). Discussions with opposing counsel and stipulations as to which computers, e-mail accounts, and archival media are relevant to the dispute will narrow the scope of data to be searched and collected.

Counsel for the requesting party may wish to depose an adversary's key IT personnel responsible for data storage, indexing, archiving, backups, computer setup (including operating system and software used), access codes and passwords, network growth and maintenance, and similar tasks. See Fed R Civ Proc 30(b)(6); CCP §2025.230. Information provided by the deposition testimony will enable the requesting party to craft a narrowly tailored request for production of electronic data that can withstand challenges based on claims of undue burden and overbreadth. Interrogatories under Fed R Civ P 33 can be useful to prepare for depositions of IT personnel.

A motion to compel may be necessary if the responding party does not cooperate in producing the requested ESI. Further, Fed R Civ P 34(a) grants the requesting party a limited right to an on-site inspection of the responding party's computer system if the responding party fails to cooperate. See §20A.38. If the responding party believes that the requesting party's demands are too vague, too burdensome, or otherwise unreasonable, the responding party may file a motion for a protective order. See generally California Civil Discovery Practice (4th ed Cal CEB 2006).

© The Regents of the University of California

B. Collecting Data

§20A.31 1. Defensible Collection Strategies

It is important that the procedures used to collect data are legally defensible, because the party whose case is weakened by the introduction of electronic data into evidence may attempt to argue that the data was altered or otherwise despoiled during the collection process. The producing party must understand how to preserve, identify, collect, and deliver the requested data without corrupting it, without disturbing normal company workflows, and without incurring exorbitant costs. In general, the producing party should:

- Enlist experienced professionals to harvest or otherwise examine data;
- Establish and maintain a legally defensible chain of custody;
- Maintain data integrity and authenticity;
- Use targeted data collection methods;
- Avoid using copy software that is "non-forensic" and changes metadata (such as the last accessed date) as it copies; and
- Preserve data carefully to avoid spoliation claims.

The producing party has a duty "to utilize the method which would yield the most complete and accurate results." *Gates Rubber Co. v Bando Chem. Indus., Ltd*. (D Colo 1996) 167 FRD 90, 112.

Counsel should seek the most effective way of processing the ESI that is economical and that produces data that is complete and usable. If the ESI produced is not complete or usable, and it would not have been cost-prohibitive to use another, more effective collection method, counsel may request that discovery be reopened at the expense of the side that failed to produce it correctly in the first place.

Data collection methods can be supported by testimony of an expert, ideally someone who has been involved with the company's operations in advance of pending litigation.

© The Regents of the University of California

§20A.32 2. Paper-Based Versus Electronic Production

Although e-mail and computer applications have been widely used for more than a decade, the majority of the data they generated for discovery was, until recently, converted to paper. The data was then scanned with optical character recognition technology or manually entered into litigation support database programs. Although scanning was generally more efficient than retyping, the document still had to be checked thoroughly for errors and missed characters, and coded or summarized. Once in the database, large volumes of documentation were queried, categorized and, where applicable, redacted before production. This process, long the standard, has proved cumbersome, costly, and duplicative.

The volume of discoverable information available today in electronic format makes conversion to paper impracticable. For example, a floppy disk with 1.44 megabytes holds more than 720 typewritten pages, while a CD-ROM containing 650 megabytes holds up to 325,000 typewritten pages. Today, with computer hard drives typically storing more than 100 gigabytes, one computer can contain more than 50 million pages of data. It would be practically impossible to print and attempt to handle that volume of data manually.

Handling production of ESI electronically can vastly increase the amount of information available for litigation. Although paper records can be lost, rendered illegible, or destroyed deliberately or inadvertently, data created and stored in a computer can be difficult to alter or delete entirely. See §20A.3. Technology now enables data to be automatically extracted and put into a format that can be seamlessly imported into a litigation review platform while still in its original "sourced" file format, *e.g.,* .wpd, .doc, or .pdf. Alternatively, the data can be converted to other formats that readily enable review. Sophisticated electronic data discovery (EDD) software can then search across formats for words, patterns of words, or concepts. See generally §20A.34. By automating and streamlining vast amounts of data, electronic document production can result in significant cost savings over the traditional paper-based process.

© The Regents of the University of California

§20A.33 3. Forensic Data Professionals

It may be advisable to have data collected by a certified forensic data professional. A forensic data collection expert normally uses state-of-the-art technology that results in a targeted and defensible data collection. Courts will look to the experience and qualifications of the expert who collects the data to ensure that there has been no spoliation or purposeful or negligent altering of the evidence collected. See *Peskoff v Faber* (D DC 2007) 244 FRD 54, 61 (qualified forensic computer technicians required in order to search computers of defendant whose consultant stated he "lacked the tools" to do comprehensive search). See also *Pension Comm. of Univ. of Montreal Pension Plan v Banc of Am. Sec.* (SD NY, Jan. 15, 2010, No. 05 CIV 9016) 2010 US Dist Lexis 1839, *10 (loss or destruction of evidence resulting from "failure to collect evidence, or the sloppiness of the review… is surely negligent, and, depending on the circumstances, may be grossly negligent or willful").

Parties who attempt to collect their own data may make four critical errors.

- Parties are often not savvy enough to collect the data without changing it or its metadata. As a result, they may despoil the data and face sanctions for evidence alteration or destruction.
- A representative of a party that collects its own data runs the risk of having to answer as an expert regarding how the data was collected and may be put in the dangerous position of being both a party and an expert witness in the same action. An attorney who is involved in hands-on data collection runs the risk of a conflict of interest if testimony on collection methods is required. An attorney usually cannot serve as a legal representative and as an expert witness in the same case.
- An inexperienced individual who attempts data collection may damage or mishandle the data source.
- A lay person may not know that it is necessary to maintain a chain of custody log or may understand the importance of one but be unable to create one that would pass muster in court.

In general, a qualified forensic data expert can:

- Search for and retrieve individual files and documents while preserving key metadata;
- Filter the data at the point of collection, thus vastly reducing the volume of data produced by collecting only potentially relevant documents and not disturbing company operations;
- Prepare declarations or be available to testify at discovery hearings; and
- Automate the collection process so that it runs around the clock on networks of any size.

Another benefit is that the forensic data expert can assist in restoring damaged files and testify regarding the probable cause of the damage. Computer files are organized on electronic devices through a file allocation table (FAT). When files are accessed, the computer looks to the FAT and finds where the file and associated data is located on the hard drive or other storage device. If a FAT gets scrambled, damaged, or destroyed, the ability to find a file and its associated data can be lost, unless a qualified forensic expert can restore the data back to its original form. Sometimes the damage is accidental, but often the forensic expert can testify concerning whether the damage or corruption was intentional. The expert may be able to pinpoint the date and time of loss. If the loss occurred after a litigation hold letter has been given, the offending party may be subject to sanctions. For discussion of litigation holds, see §20A.25.

© The Regents of the University of California

§20A.34 4. Electronic Data Discovery Software

In general, there are two ways to collect data using specialized forensic collection software: (1) full disk imaging and (2) targeted forensic collections.

- A full disk image is an electronic copy of every bit and byte of a computer, including system files and all user-created files, regardless of whether they are relevant to the scope of the discovery request. See §20A.37 for further discussion of this technique and when it may be used.
- Forensic data collection is a less time-consuming and less costly targeted collection in which specialized software is used to "dig out" only the user-created files requested.

Forensic data collection software (also known as electronic data discovery (EDD) software) can help limit the amount of data that must be reviewed. It can scan a large network infrastructure, search across multiple file formats including e-mail, and then filter at the point of collection, allowing the system to collect only data that has been prescreened by key word, word proximity or concept, date, date range, file type, or author or recipient (or any combination thereof). This technology can strip out system files, duplicate data, and then, based on culling criteria, retrieve specific files from the target network. It is able to scan the files without changing any of the underlying metadata. It can also collect data concurrently from multiple machines by harnessing new technology known as "multi-threading." Thousands of computers at a corporate headquarters, for example, can be simultaneously mined for certain requested e-mail messages, spreadsheets, and word processing documents. This process is a nonintrusive one that allows computer users to continue to work at their computer as usual. A litigant can thereby capture, quickly and cost-effectively, only the data potentially relevant to the issue at hand. For example, the software can gather all e-mails between certain parties authored within a certain date range, perhaps containing certain words or phrases, without expending the cost and time of collecting and reviewing the entire drive.

NOTE: It is important to choose an EDD vendor that can provide National Institute of Standards Technology certification of the software's ability to forensically extract and examine the data without disturbing it.

An understanding of how the computer stores and retrieves data is essential to understand what is being extracted and saved. An attorney who utilizes EDD software but does not understand how the process works is in danger of missing out on important data or being unable to judge whether an EDD vendor has done its job to the required specifications and if the work product will "stand up" in court.

© The Regents of the University of California

§20A.35 5. Risks in ESI Collection

Parties must use caution when collecting electronic data. Although it may seem quick and easy to, *e.g.,* log on to a computer, look at what it contains, and pick and choose what to "grab," doing so is unwise. It is also unwise to load an e-mail file onto another computer to take a quick look at it. Because the simple act of opening a file changes several metadata fields (see §20A.36), some of which could be critical to the case, the "quick look" may irretrievably alter the data and result in sanctions for altering data that has been reviewed. For this reason, methods of collection that alter metadata should be strictly avoided unless expressly approved by opposing counsel or the court. There is an additional risk that a virus may infect the files being reviewed.

CAUTION: In particular, counsel and parties should avoid collecting e-mail by forwarding the e-mail or dragging and dropping it into a folder, because doing so changes the metadata. Moreover, a quick look at e-mail, whether on the client's computer or on counsel's own, creates a risk that any e-mails stored in the outbox will be sent (an automatic feature of most e-mail systems).

© The Regents of the University of California

§20A.36 6. Metadata

Electronic data contains information known as "metadata" that paper data does not provide. Metadata is "data about data"—it provides information about everything that happens to a document, such as when the document was accessed and by whom, when was it modified, how many times was it accessed, and which version was e-mailed and to whom. Metadata allows access to older versions of the document and previous revisions of that document if those items were not erased prior to notification of litigation.

Some metadata is very easily changed. The simple act of turning on a computer and opening a file can change the number of different metadata fields within the computer. Once the metadata has changed, there is often no way to restore the document to its previous state. On the changeable nature of metadata, see *Williams v Sprint/United Mgmt. Co.* (D Kan 2005) 230 FRD 640, 646 (metadata can be changed intentionally or inadvertently). The changeable nature of metadata makes it essential that attorneys and parties delay collection of electronic data in a litigation matter until after they have sufficient knowledge about whether metadata could be important to the case (*e.g.,* whether there may be a dispute about when a document was created), and whether the parties must therefore preserve the metadata or include metadata in the materials to be produced.

NOTE: Attorneys who ignore metadata in the documents produced may miss important information that may be critical to their case. Likewise, attorneys who fail to review the metadata they are providing to opposing counsel may face liability, or at least be put in an awkward position when dealing with opposing counsel.

Bar associations and states have issued conflicting ethics opinions on how attorneys should deal with metadata. The ABA has stated that lawyers who receive ESI from opposing counsel as part of discovery document production are free to look for and examine metadata that arrives with the documents. ABA Formal Opinion 06-442 (Aug. 2006). The District of Columbia is among the jurisdictions that have followed the ABA opinion, finding that a lawyer is prohibited from reviewing metadata in records produced by an adversary "only when [the lawyer] has actual knowledge that the metadata was inadvertently sent." DC Legal Ethics Comm Op 341 (Sept. 2007). These opinions run contrary to ethics opinions out of New York and Florida, which have opined that metadata mining—an affirmative act on the part of the receiving lawyer—is generally unethical. NY Comm on Prof Ethics Op 749 (Dec. 14, 2001); Florida Bar Prof Ethics Op 06-2 (Sept. 2006). A current summary of metadata ethics opinions by jurisdiction is available at http://www.abanet.org/tech/ltrc/fyidocs/metadatachart.html.

For further discussion of handling metadata, see §20A.43.

© The Regents of the University of California

§20A.37 7. Forensic or Mirror Images

A forensic image (or mirror image) is an exact copy (bit for bit) of a hard drive. This kind of image of a hard drive captures all deleted files and slack space as well as all active data. (Slack space is empty space that cannot be used, but may contain remnants of deleted files.) Creating a forensic image of a drive ensures that the client has gathered all of a computer user's data. It provides visibility into all communications generated on the computer in question, including file copying, deletion, or other unusual activity. A fully imaged drive allows the attorney to view desktop items and folder and subfolder structures in the same way that the computer's original custodian may have done.

Forensic images are often used in criminal matters and quasi-criminal regulatory matters. They are also frequently used in employment matters in which there is the possibility of theft or destruction of intellectual property or the abuse of company policies, or when an employee has left under contentious circumstances. Whether to use forensic imaging must be determined by the need for preservation in each case. In some cases, although it may be necessary to create a mirror image of a hard drive, it may not be necessary to process (*i.e.*, manipulate) the data on that hard drive. In fact, the report that is generated by the forensic process can provide great insight about what is on the drive and can be used as a tool to decide what needs to be processed. In most of the cases requiring forensic imaging, it is usually only necessary to take a mirror image of the hard drives of a few key data custodians.

In litigation involving thousands of computer users and multiple offices and networks, a full image of all systems (or even some systems) may be impractical and the cost prohibitive. This is especially true if the scope of the ESI at issue can be narrowed based on criteria such as custodian, file type, date range, or even key word or phrase. Discovery in such litigation lends itself well to a "targeted" collection using special software to "sniff out" the relevant files across vast networks and among multiple machines and collect only specific relevant files.

NOTE: Some IT professionals use the terms "mirror" and "ghost" interchangeably. There is, however, a crucial distinction between these two operations when data is being gathered. Unlike mirroring, the ghost process generally involves copying only live files and their associated metadata and thus can be misinterpreted as being a "mirror image" when in fact it is not. Counsel should forestall any misunderstanding by making clear to those collecting the data which operation is desired.

© The Regents of the University of California

§20A.38 8. Right to On-Site Inspection

On-site inspections of an opponent's computer systems, although rare, are permitted under both the federal rules and the Electronic Discovery Act. See Fed R Civ P 34(a); CCP §2031.010. Both authorities allow for an on-site inspection of a party's computer or other media. See §20A.13. There is a developing body of case law addressing how and when an adverse forensic examination or on-site inspection may proceed. Federal courts have historically resisted such incursions. In *Diepenhorst v City of Battle Creek* (WD Mich, June 30, 2006, No. 1:05-cv-734) 2006 US Dist Lexis 48551, the requesting party was denied a forensic examination consisting of making a mirror image of the responding party's hard drive, on grounds that the requesting party had not shown that the responding party had destroyed evidence or had otherwise failed in its discovery obligations. See also *Powers v Thomas M. Cooley Law School* (WD Mich, Sept. 21, 2006, No. 5:05-cv-117) 2006 US Dist Lexis 67706 (discussing Ford in light of then-proposed, now-adopted comment to Fed R Civ Proc 34). But see *Advante Int'l Corp v Mintel Learning Technol.* (ND Cal, Nov. 21, 2006, No. C 05-01022 JW) 2006 US Dist Lexis 86334 (examination of responding party's hard drive ordered after evidence indicated alteration of requested e-mails).

After the amendments to Fed R Civ P 34(a), the judicial standards for gaining access to an adversary's computer infrastructure may become less restrictive, although the Advisory Committee's notes caution that Rule 34(a) was not intended to create a routine right of direct access. See §20A.13. When counsel suspects the other side is engaging in questionable tactics and there is a reasonable fear that ESI could be altered or destroyed, Rule 34(a) can be a powerful tool, not only to stop destruction of ESI but also to preserve it intact on the systems on which it was created.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/20A Discovery of Electronically Stored Information/ §20A.39 C. Form of Production

§20A.39 C. Form of Production

The form of production of electronically stored information is subject to much debate. As acknowledged by Cal Rules of Ct 3.724(8) and Fed R Civ P 26(f)(3)(C), arriving at an agreement on an acceptable format for production is critical to planning electronic discovery. Generally, data is exchanged in image format supplemented with a metadata file, or in native format. Under the federal rules, absent an agreement to the contrary, ESI is to be delivered in the format in which it is normally stored, which is invariably a native format (*e.g.,* Word documents are produced as .doc files and not as images or .pdf renditions of the document). See Fed R Civ P 34(b)(2)(E).

© The Regents of the University of California

§20A.40 1. Production in Native Format

"Native" refers to the original electronic file in its original format. For example, if an original document was created with a word processing program such as Word or WordPerfect, to produce the document in native format would mean producing a copy of the original Word or WordPerfect file in Word or WordPerfect, as the case may be, and not converting the document to another file format. As discussed in §20A.14, under both the Electronic Discovery Act (see CCP §§1985.8(c)(1), 2031.280(d)(1)) and Fed R Civ P 34(b)(2)(E), documents must now be produced in their native format unless the requesting party specifies another format.

Production in native format, as required by both federal and California rules, represents a departure from current litigation practice. Historically, ESI was simply printed out and produced in a paper hard-copy format. More recently, electronic records have been converted to, and produced in, digital image formats such as .tiff, .jpeg, .gif, .bmp, or .pdf. Converting native files to paper or image formats can prove costly and time-consuming, however. Rule 34(b) was intended to simplify and speed up the process of production of ESI, as well as to reduce costs. As discussed in §20A.43, production of ESI in native format also preserves the metadata associated with each document and helps defeat claims that a document has been altered or that metadata has been changed or hidden with a change in file format.

There are drawbacks to producing or receiving native documents, such as the difficulty of numbering the documents. Traditionally, when paper documents are produced, the parties will affix a control number. With native documents, however, to add a control number to every page is to change and thus spoil the document. As a result, the usual practice is to assign one control number to the entire document instead of a number to each page within the document.

NOTE: It is possible to use a method called the "MD5Hash value" as the control number for native documents. MD5Hash (which stands for "Message-Digest algorithm 5 with a 128-bit hash value") is a formula used to create a digital signature that is specific to each file and document and constitutes a document's electronic fingerprint. The hash value is generated on the basis of the total content of the document. Like a human fingerprint, no two documents have the same MD5Hash value. Use of a newer standard, SHA (Secure Hash Algorithm), which is similar to the MD5Hash methodology for identifying unique electronic documents, is becoming more common. The SHA hash functions represent five cryptographic hash functions designed by the National Security Agency (NSA) and published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS).

Another drawback to receiving native files is that they must be imported into a platform (*i.e.*, a computer or operating system with necessary application software) in order to be reviewed. This can be costly and cumbersome, depending on what tools the reviewing party has at hand. For example, the reviewing party might not have access to the software application needed to review a particular native file. As a result, the costs associated with processing native files for review can tip the scales in a litigation budget. Moreover, there are often situations where the necessary software was created by a company that no longer exists, or the necessary software has been uninstalled and the source disks thrown out years ago, or the software has been upgraded to a point where the original data can no longer be accessed in its original format. On the other hand, users with access to advanced litigation support databases are likely to be able to ingest the native files directly into the database and begin review without the added traditional steps of scanning, OCR, and human coding of all information.

PRACTICE TIP: When faced with outdated software or systems (so-called "legacy" systems), it may be possible to purchase software at an online auction site in order to read the data in its original format. Also, it is possible to purchase "file viewing" software that allows opening and viewing native documents even if the underlying software application is not installed or is not running.

© The Regents of the University of California

§20A.41 2. Production of Image Files

An image file is a copy of all or part of a hard drive, floppy disk, program, or data and is often in .tif or .tiff (Tagged Image File Format) or .pdf (Portable Document Format). When producing images of electronically stored information containing metadata, a party provides a scanned reproduction or image of every page of every document as well as the metadata associated with the file. The image file, usually produced on disc or tape, is essentially an electronic version of the boxes of paper documents that change hands during paper discovery. The main difference between production of images and paper document production is that additional important information (the metadata) is possibly produced along with the documents. It is important to remember that data can be "burned" to a static format such as .tiff, .pdf, or .gif and stored on a CD, DVD, or hard drive for production to the requesting party in lieu of the production of an image of the media. Little to no metadata will be present with such a static format beyond some information about the static file itself. The benefits and pitfalls of a static production are discussed further in §20A.42.

NOTE: As discussed in §20A.14, under Fed R Civ P 34(b) as amended, documents cannot be produced in an image format unless the requesting party consents.

© The Regents of the University of California

§20A.42 a. Copying Electronic Files

In *Hagenbuch v 3B6 Sistemi Elettronici Industriali SRL* (ND IL, Mar. 8, 2006, No. 04 C 3 109) 2006 US Dist Lexis 10838, the court agreed with the requesting party that requested data produced in .tiff format was not a satisfactory substitute for copies of the electronic media. The requesting party argued that the .tiff images were found to (2006 US Dist Lexis 10838 at *4):

> (1) lack clarity and color, (2) lack metadata that track when a document was created or modified and whether e-mails contained attachments and to whom they were sent, (3) lack clear indications as to where each document starts and stops (i.e., the TIFF pages all run together and make it difficult to determine which pages are part of one document), (4) lack clear indications as to which documents are stored together on the original compact discs and DVDs (i.e., over sixty original compact discs and DVDs were reduced to four compact discs containing TIFF documents), and (5) make it impossible for Plaintiff to use search terms to quickly and efficiently search through the documents electronically.

The responding party argued that the provision in Fed R Civ Proc 34(b)(2)(E) requiring a party to produce documents as "kept in the usual course of business" to applied to the form in which the documents were organized, not the form of the documents themselves. The responding party argued further that the .tiff documents produced were "in reasonably usable form," and therefore in compliance with the statute. The court disagreed, and ordered the responding party to produce copies of the electronic media in the form identified and requested by opposing counsel.

© The Regents of the University of California

§20A.43 b. Handling Metadata

How much metadata must be produced varies from case to case, and there are differing views concerning what is required. For example, in *Williams v Sprint/United Mgmt. Co.* (D Kan 2005) 230 FRD 640, 652, the court ordered the defendant to produce Excel worksheets with the metadata, stating that:

> [W]hen a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order.

See also *Hagenbuch v 3B6 Sistemi Elettronici Industriali SRL* (ND IL, Mar. 8, 2006, No. 04 C 3 109) 2006 US Dist Lexis 10838 (.tiff files unacceptable without metadata).

The basic principle is that documents produced in response to an inspection demand must be produced "as they are kept in the usual course of business" or be organized and labeled to correspond with the categories in the request. See CCP §2031.280(a); Fed R Civ P 34(b)(2)(E)(i). Arguably, data as it is kept in the usual course of business means data is produced with the metadata intact, not stripped of it. See *Nova Measuring Instruments Ltd. v Nanometrics, Inc.* (ND Cal 2006) 417 F Supp 2d 1121 (documents must be produced in native format, with metadata intact), citing *In re Verisign Secs. Litig., Inc.* (ND Cal, Mar. 10, 2004, No. C 02-02270 JW) 2004 US Dist Lexis 22467 ("documents need only be produced in their native format, *i.e.,* in the format that they were stored during Defendants' usual course of business"). As a practical matter, however, the definition of "ordinary course of business" may vary with the parties and the presiding judge.

A party is not obligated to produce electronic documents with metadata if the initial discovery request does not ask for it. *Autotech Technols. LP v AutomationDirect.com, Inc.* (ND Ill 2008) 248 FRD 556, 560. See also *In re Payment Card Interchange Fee & Merchant Discount* (ED NY, Jan 12, 2007, MD 05-1720 (JG) (JO)) 2007 US Dist Lexis 2650 at *4 (parties need not reproduce documents already produced to include metadata, but must produce metadata for any documents not yet produced). But see *Williams v Sprint/United Mgmt. Co.* (D Kan 2005) 230 FRD 640, 652 (metadata should be produced by party aware or reasonably aware that particular metadata is relevant to dispute).

Even if the metadata need not be produced in every case, it should be preserved. See *Pueblo of Laguna v U.S.* (2004) 60 Fed Cl 133 (government required to preserve all documents, including metadata, that contained relevant information or that might lead to discovery of relevant information).

© The Regents of the University of California

§20A.44 D. Privileged Information

The vast amount of data on computer systems renders it nearly impossible to thoroughly review electronically stored information before production. As a consequence, the risk of inadvertent production of data subject to the attorney-client privilege or work product protection has increased. As noted in §20A.9, the new rules take this risk into account and soften the penalties for erroneous production of privileged material.

Both the Electronic Discovery Act (see CCP §§1985.8(i), 2031.285) and Fed R Civ P 26(b)(5)(B) set forth default procedures for retrieval of inadvertently produced ESI, which is operative unless the parties agree on another framework for dealing with the issue. Following the procedure, the inadvertent production may be excused and the data retrieved with no detriment to the producing party. If privileged information is inadvertently produced:

- The producing party must notify the recipient and state the basis for retrieval claim;
- The recipient must promptly return, sequester, or destroy the specified information upon notice that data was inadvertently produced;
- The recipient may not use or disclose the information until the inadvertent disclosure claim becomes resolved;
- If the receiving party disclosed subject information prior to notification, it must take reasonable steps to retrieve it; and
- The producing party must preserve subject information until claim resolved.

This "clawback" provision allows a party who accidentally produces any privileged matter when supplying ESI to notify the other party and have it isolated and not used until judicially reviewed.

© The Regents of the University of California

§20A.44A E. Federal Rule of Evidence 502

Federal Rule of Evidence 502 is a new evidentiary rule concerning the attorney-client privilege and work product doctrine. One element of the rule is particularly germane to electronic discovery: namely, the provision that negates any waiver of the privilege if disclosure of privileged information in a federal proceeding was inadvertent and the producing party took reasonable steps to prevent the disclosure from occurring and takes prompt and reasonable steps to rectify the error. If the producing party complies with the rule, the limitation on waiver of the privilege is operative in both federal and state proceedings. Fed R Evid 502(b). See also Fed R Evid 502(c) (reciprocal rule for inadvertent disclosure of privileged information in state proceedings). Given the vast amounts of data that must be managed during the electronic discovery process, there is a high likelihood that privileged materials may be inadvertently produced.

It is important to note that Fed R Evid 502(b) does not permit counsel simply to turn over *all* discoverable information to the requesting party in order to save time and money and thereby bypass the need for a labor- and cost-intensive review for privilege on a document-by-document basis.

- The benefits of the rule apply *only* to counsel who *inadvertently* produce privileged materials, and not to counsel who *purposefully* turn over privileged documents to opposing counsel. See Fed R Evid 502(b)(1).
- An attorney who produces privileged documents in reliance on the availability of a limitation on waiver must be able to show that he or she took "reasonable steps" to prevent inadvertent production. If production of privileged material was intentional, this prong of the rule will not be satisfied. See Fed R Evid 502(b)(2).
- Under the rule, counsel has an obligation to take "reasonable steps" to cure inadvertent production of privileged material. It would be difficult for counsel to claim that he or she took reasonable steps to rectify inadvertent production of privileged material if counsel's intention was in fact to produce all material. See Fed R Evid 502(b)(3).

Rule 502 does not define what constitute "reasonable steps" to prevent inadvertent disclosure; however, courts addressed the issue before enactment of the rule. See, *e.g., Victor Stanley, Inc. v Creative Pipe, Inc.* (D Md 2008) 250 FRD 251, 262 (finding waiver where search of electronic files using approximately 70 keywords was not "reasonable precaution" against inadvertent disclosure). See also *Rhoads Indus., Inc. v Building Materials Corp. of Am.* (ED Pa 2008) 254 FRD 216, 220 (noting other factors for court to consider in assessing reasonableness of precautions, including number of documents claimed to have been inadvertently produced). But see *Heriot v Byrne* (ND Ill 2009) 257 FRD 645, 655 n7 (criticizing *Rhoads* for resolving the waiver question by ignoring Fed R Evid 502 in favor of test articulated in *Judson Atkinson Candies, Inc. v Latini-Hohberger Dhimantec* (7th Cir 2008) 529 F3d 371, 387, essentially "substitut[ing] judicial holdings for legislation").

Regarding what constitute "reasonable steps" to rectify counsel's error, Fed R Evid 502(b)(3) indicates that notifying opposing counsel of the privilege claim and the basis for it, in accordance with Fed R Civ P 26(b)(5)(B), would constitute a "reasonable step," among possible others.

NOTE: Even if a producing party can meet the tests of Rule 502(b) and can rely on the continued availability of the privilege, the fact remains that the disclosure revealed confidential and possibly damaging information to the opposition. Savvy opposing counsel might find ways to use this information against his or her adversary without presenting it directly on the record. Moreover, Rule 502 does not allow attorneys to circumvent their obligation to review discoverable evidence on a document-by-document basis for relevance, responsiveness, national security issues, trade secrets, and other characteristics that do not pertain to privilege.

© The Regents of the University of California

F. Data Processing, Storage, and Review

§20A.45 1. De-Duplication

Once data has been collected ("harvested"), it ordinarily needs to be processed so that it can be imported into a litigation support database (see §20A.46) and the data, metadata, and document images can be made available for categorizing, querying, redaction, numbering, and production. There are many commercial vendors that will convert harvested data to a load file format for specialized litigation support programs in .edii load file format, .dcb format, or .log format.

The processing of data involves the conversion of the data into a format that can be harnessed by litigation support databases. As part of the process, the raw data will be "de-duplicated"—*i.e.,* duplicate copies of documents or e-mail will be removed, by "hash code" or SHA technology. See §20A.40. The ability to identify exact duplicates based on "hash values" often reduces the volume of material to be reviewed by as much as 25 percent.

De-duplication can be horizontal (across the data of multiple custodians) or vertical (within the data of a single custodian). Horizontal de-duplication removes far fewer records, but keeps intact the population of records gathered for each custodian. Some processes also offer "near de-duplication," which suppresses earlier e-mails within an e-mail chain and retains only the last, most complete message for review. There are also technologies available that group all near-duplicates together so that they can all be reviewed together. De-duplication does not eliminate metadata concerning duplicates, such as who received the same message and when they received it.

Throughout the data processing phase, the data is not only de-duplicated, but it is also "cracked open" and the metadata is collected and optimized to be exported into a review platform so that interested parties can evaluate it.

© The Regents of the University of California

§20A.46 2. Litigation Support Platforms

A database designed specifically for use with discovery data is an important litigation support tool. Most litigation support platforms or databases will uniquely number and store records, each of which is a discovery document, and each of which may contain information about the document such as document type, date, creation date, revision dates, topic, author, and recipient, which was pulled from the electronic document during the data processing phase and put into specific fields. The fields are automatically pulled from the electronic document by manual or automatic coding. The documents may also be converted to a .tiff image format so that they can be viewed like pictures within the review platform. See §20A.41. Attorneys can redact the images if desired, and turn them into trial exhibits by marking them up with arrows or highlighters usually available within the review platform application.

The platforms often include data sampling capabilities, which allow a representative sample of a large volume of data to be surveyed for relevance, further helping to limit overproduction and its attendant time and expense. For a premium, newer platforms allow automated clustering of similar electronic files based on new technologies known as "concept engines" that compare the contents and relationships between files such as e-mail and sort similarly themed files together to enhance review workflow.

A new breed of "early case assessment" platforms allows a user to look at a particular document and code it by categorizing it as privileged or nonprivileged and indicating what issues the document may help prove or disprove. The platform can automatically find all similar documents in a large population and "bulk code" those documents in the same fashion. This allows automatic categorization of documents without the need for a reviewer to actually view all of the documents; thus, the user can concentrate on important subsets of the categorized document population as needed at a later date. Courts have accepted this methodology of categorization when the reviewer can "sample"' a batch of documents for the court and show that the batch has been adequately categorized.

© The Regents of the University of California

§20A.47 3. Hosting

To "host" data means to provide data storage, software, and other services to client computers that connect from remote locations, *e.g.,* from the computers of experts or co-counsel or from different computers within the same firm. Before counsel decides to host the data that has been collected and processed, whether within the firm's network or on a third party data-hosting service, it is important for counsel to consider the following:

- To support hosting, the computer infrastructure must have, *e.g.,* the necessary servers (computers that control access to a network or its resources), bandwidth (data transfer capacity or transmission speed), connectivity (ability to transmit data between devices), and security;
- The infrastructure must support multi-office reviews;
- The infrastructure must be capable of sharing data with co-counsel, experts, or clients;
- The costs of hosting;
- The security of data as it resides on a third party network that is broadcast over the Internet;
- Staff must be available to load data into the database and support the users; and
- Whether there are options other than hosting.

Several "off-the-shelf" applications and customizable applications can be used if counsel decides to host data internally. Regardless of which application is selected, because the application will play a vital part in the discovery process, counsel must be sure to have the software vendor's full support. Even the best in-house litigation support professional will not be able to solve every problem and will need to turn to the software company for a rapid solution. Should counsel decide not to host the data internally, there are many reliable application service providers (ASPs) and forensic consulting companies that can host the data.

PRACTICE TIP: There are many benefits in using an ASP, the most important of which is that an ASP usually provides round-the-clock support and seamless collaboration possibilities.

© The Regents of the University of California

§20A.48 4. Data Security

Discovery data must be kept safe—physically as well as electronically. The server containing the data must be in a safe and secured location. For example, many law firms and ASPs (application service providers) have biometric (palm print or retina scan) keycard or keypad security along with cameras on the door to the "server room." Most server rooms are also equipped with fire safeguards in case of a fire. Removed hard drives and backup tapes should be stored in fireproof safes regardless of the building's fire safeguards. Electronic safety is just as important. Counsel must make sure that the data has the highest level of encryption and firewall protection. Often counsel will be reviewing data that is not only crucial to the case but that also contains highly confidential information. Counsel must be sure that the strongest precautions are taken to safeguard client data. Backups should be made frequently, and a copy of the backups should be stored off-site for protection in the event of a catastrophe.

© The Regents of the University of California

§20A.49 G. Costs of E-Discovery

A highly contested area of electronic discovery revolves around costs. Most litigation professionals realize that the cost of electronic discovery pales in comparison to the huge costs associated with paper management and production. Nevertheless, cost is always a relevant factor.

Courts in numerous jurisdictions have considered whether the requesting party or the responding party pays should assume the cost of electronic discovery.

In *Toshiba Am. Electronic Components, Inc. v Superior Court* (2004) 124 CA4th 762, 21 CR3d 532, the court of appeal held that CCP §2031.280(c) (former CCP §2031(g)) is a legislatively created exception to the rule that the responding party is responsible for the costs of responding certain discovery requests. Under CCP §2031.280(c) (former CCP §2031(g)(1)), the requesting party must bear the reasonable expense of translating a requested data compilation into useable form for discovery.

Federal courts, however, generally follow the cost-splitting scheme set forth in *Zubulake v UBS Warburg LLC* (SD NY 2003) 216 FRD 280. The *Zubulake* court held that the following factors should be considered to address cost-shifting in the discovery of inaccessible data (216 FRD at 284):

- The extent to which the request is specifically tailored to discover relevant information;
- The availability of such information from other sources;
- The total cost of production, compared to the amount in controversy;
- The total cost of production, compared to the resources available to each party;
- The relative ability of each party to control costs and its incentive to do so;
- The importance of the issues at stake in the litigation; and
- The relative benefits to the parties of obtaining the information.

The court stated that the factors should be "weighted more-or-less" in the order in which they are listed. 216 FRD at 284.

In determining whether the requesting party's need for discovery outweighs the burden on the responding party, the court also has the authority to consider whether the requesting party is willing "to share or bear" the cost of obtaining information deemed "not reasonably accessible." Advisory Committee Notes, 2006 Amendment to Fed R Civ P 26.

© The Regents of the University of California

21

International Issues

I. INTERNATIONAL E-BUSINESS ISSUES
- A. Introduction §21.1
- B. Hague Conference on Private International Law §21.2
- C. Applicable Law in International Disputes §21.3
- D. Jurisdiction of Foreign Courts §21.4
- E. Comity: Enforcing Foreign Judgments Against U.S. Companies §21.5
- F. Content Filtering by Foreign Governments §21.6
- G. How to Target or Not Target Certain Countries §21.7
- H. International Electronic Contracting §21.8
- I. International Intellectual Property Protection §21.9
- J. European Union Directives
  - 1. Introduction §21.10
  - 2. EU Data Protection Directive
    - a. Generally §21.11
    - b. Compliance With EU Data Protection Directive
      - (1) Safe Harbor Certification §21.12
      - (2) Case-by-Case Compliance; Model Contract Clauses §21.13
  - 3. Other EU Directives
    - a. Distance Selling §21.14
    - b. E-Commerce Directives §21.15
    - c. VAT Directive §21.16
    - d. Specific Industry Directives §21.17
    - e. EU Privacy Directive §21.18
    - f. EU Data Retention Directive §21.18A
- K. Self-Regulation
  - 1. Trustmarks §21.19
  - 2. International ADR §21.20

II. EXPORT CONTROLS ON COMMERCIAL SOFTWARE AND TECHNOLOGY
- A. Introduction §21.21
- B. Export Control Analysis §21.22
  - 1. Transactions Subject to Export Controls §21.23
  - 2. Definition of "Export" §21.24
  - 3. Fines and Penalties for Violations §21.25
- C. Product Classification §21.26
  - 1. Commerce Control List (CCL); Export Control Classification Number (ECCN) §21.27
  - 2. Country Chart §21.28
  - 3. Software Without Encryption
    - a. Publicly Available Software §21.29
    - b. Object Code or Source Code §21.30
    - c. Software Incorporated in Computer Hardware §21.31
  - 4. Software With Encryption §21.32
    - a. "Limited" Encryption Software Requiring Prior Review §21.33
    - b. "Full" Encryption Software Exempted From Prior Review
      - (1) Limited Cryptography §21.34
      - (2) Ancillary Cryptography §21.34A
      - (3) Other Wireless Encryption Items §21.34B
  - 5. Classification Procedures §21.35
- D. Development, Distribution, and Sales §21.36
  - 1. General Rules
    - a. Software Without Encryption §21.37
    - b. Software With Encryption §21.38
      - (1) U.S. Subsidiaries §21.39
      - (2) "Prohibited" Countries §21.40
      - (3) "Preferred" Countries §21.41
      - (4) "Permitted" Countries §21.42
      - (5) "Retail" Encryption Items **[Deleted]** §21.43

c. "Cryptanalytic" Items §21.44
2. Special Rules
a. Beta Test Software §21.45
b. Encryption Source Code §21.46
c. Publicly Available Source Code §21.47
d. Related Technology §21.48
E. Compliance Measures §21.49
1. Knowledge of Export Control Violations §21.50
a. Knowledge of Ultimate Destination §21.51
b. Prohibited End Users §21.52
c. Prohibited End Uses §21.53
2. Export Transaction Documentation
a. Automated Export System Record §21.54
b. Destination Control Statement §21.55
c. Contractual Certifications §21.56
d. Website Screening System §21.57
e. Access Control System §21.58
3. Reporting and Recordkeeping
a. Encryption Exports Reports §21.59
b. Records Maintenance §21.60
4. Export Control Compliance Program §21.61

© The Regents of the University of California

I. INTERNATIONAL E-BUSINESS ISSUES

§21.1 A. Introduction

Sections 21.2-21.20 present an overview of some international issues of interest to companies doing business on the Internet, a global marketplace. While an Internet website can provide access to a vast potential market, it can also result in exposure to expensive and inconvenient litigation under a multitude of legal systems. The recent efforts of the Hague Convention on Private International Law to draft rules to govern international jurisdiction and enforcement of judgments are reviewed in §21.2. The topics of applicable law in international disputes, foreign court jurisdiction, and enforcement of foreign judgments against U.S. companies are considered in §§21.3-21.5. Content filtering by foreign governments, such as China, is reviewed in §21.6. Section 21.7 suggests ways to target, or to avoid targeting, certain foreign countries in online operations. International electronic contracting and international intellectual property protection are discussed in §§21.8-21.9.

The United States has been a leader in the development of the Internet as an uncensored, freewheeling marketplace for goods and information, but American companies doing business online are now facing e-commerce regulations of other nations, particularly the European Union. European Union directives that may affect U.S. companies doing business online are discussed in §§21.10-21.18. International efforts promoting self-regulation online are reviewed in §§21.19-21.20.

PRACTICE TIP: In many cases, online transactions can be structured to minimize exposure to liability under foreign law, although it may be advisable to employ local counsel to assist in this process.

Sections 21.21-21.61 discuss United States export controls, a topic of particular concern to U.S. companies engaged in online transfer, sale, or distribution of software overseas.

© The Regents of the University of California

§21.2 B. Hague Conference on Private International Law

The extent to which a company doing business on the Internet from a base in the United States may be subject to the laws of foreign nations and liable for judgments rendered abroad is often uncertain. To address this uncertainty for its member states, the Hague Conference on Private International Law adopted a Convention on Exclusive Choice of Court Agreements (the Convention) on June 30, 2005, to govern jurisdiction and enforcement of judgments among its 69 member states, which include the United States as well as European, African, South American, and Asian nations. The Convention does not apply to business-to-consumer contracts, employments contracts, or contracts on certain other specified subjects. It establishes rules for enforcing agreements between parties regarding the forum for resolution of disputes and rules for recognizing and enforcing the decisions issued by the chosen forum. See the full text of the Convention at http://www.cptech.org/ecom/jurisdiction/text06302005.pdf.

Under the Convention, the court chosen by the contracting parties would hear the case, all other courts would decline jurisdiction, and member states would recognize and enforce a judgment rendered by the designated court. See Articles 5 and 6. The provisions of the Convention are broad enough to apply to nonconsumer browse-wrap and click-wrap agreements, as long as they are documented by a "means of communication which renders information accessible so as to be usable for subsequent reference." See Article 3(c).

© The Regents of the University of California

§21.3 C. Applicable Law in International Disputes

Notwithstanding the borderless marketplace in which online businesses operate, a nation may prescribe laws governing conduct that "wholly or in substantial part, takes place within its territory." Restatement (Third) of the Foreign Relations Law of the United States §402(1)(a). The protections available to online businesses under U.S. law may not be available to their operations in foreign countries, even when the act resulting in injury originated in the United States. For example, the British High Court refused to apply protections available to ISPs under U.S. law when it held an ISP liable for the publication of allegedly defamatory statements that originated with a third party in the United States. See *Godfrey v Demon Internet Ltd.* (1999) 4 All ER 342 (QBD), (2000) 3 WLR 1020, (2001) QB 201, in which the court held that the defendant, a British Internet service provider, published defamatory material originally posted on an American server by transmitting it, thus making it accessible to British subscribers. A copy of the *Godfrey* decision is posted at http://www.cyber-rights.org/documents/godfrey_decision.htm.

In a widely reported case, French law was applied to prosecute Yahoo! Inc. in France for providing French users with access to Nazi-related material and auctions of Nazi memorabilia—a violation of a French law prohibiting exhibition or sale of items deemed to incite racial hatred. See *UEJF et La Licra v Yahoo! Inc. et Yahoo France*, Tribunal de Grande Instance de Paris (Nov. 20, 2000), available at http://www.juriscom.net/txt/jurisfr/cti/yauctions20000522.htm. The court ordered Yahoo! to block French citizens' access to its offending sites or face fines for noncompliance. See §21.5 for discussion of the related U.S. case.

At least one U.S. court has rejected the application of foreign law in a case involving a Spanish company doing business online that consented to U.S. jurisdiction. In *Barcelona.com v Excelentisimo Ayuntamiento de Barcelona* (4th Cir 2003) 330 F3d 617, the Fourth Circuit reversed the district court decision applying Spanish law because the plaintiff, claiming rights to a domain name under Spanish law, had agreed to be subject to jurisdiction in the United States where the contested domain name was registered, thus opening the way for a claim under U.S. law.

Conversely, in *Zheng v Yahoo! Inc*. (ND Cal, Dec. 2, 2009, No. C-08-1068 MMC) 2009 US Dist Lexis 111886, the federal district court ruled that U.S. law—here, the Electronic Communications Privacy Act of 1986 (ECPA) (see §§18.8-18.10)—did not apply to the interception, acquisition, or disclosure of electronic communications outside the United States, even if the communications at issue had traveled through networks within the United States. In *Zheng,* the court dismissed the claims of three Chinese nationals living in the Unites States that Yahoo! violated the ECPA by intercepting and accessing e-mails in China and disclosing the e-mails along with related user information to the Chinese government.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/21 International Issues/§21.4 D. Jurisdiction of Foreign Courts

§21.4 D. Jurisdiction of Foreign Courts

Online business activities that have a substantial effect in a particular country may provide a basis for the jurisdiction of that country's courts. See Restatement (Third) of the Foreign Relations Law of the United States §402, Comment d. Recent cases illustrate the tendency of foreign courts to uphold the jurisdiction of the forum where effects are felt and damages occur, regardless of the nationality of the defendant.

An Australian Internet case illustrates application of this "effects doctrine." In 2002, the Australian High Court found that an Australian businessman could bring a libel action in a local Australian court against Dow Jones & Co., Inc., an American company, for allegedly defamatory material published in the online version of Barron's, despite the fact that Dow Jones' website originated from New Jersey. See *Dow Jones & Co. v Gutnick* [2002] HCA 56 (10 Dec 2002), available online at http://www.austlii.edu.au/au/cases/cth/HCA/2002/56.html. The court found that the allegedly defamatory material was "published" in Australia because it was downloadable by paid subscribers there, that the tort was therefore committed in Australia so that Australian law applied, and that Dow Jones had accepted the risk of being sued in Australia by accepting paid subscriptions from Australian residents.

In a similar case, allegedly defamatory remarks about Harrods, a British business, published in print only in the U.S. edition of the Wall Street Journal but available online in Britain, subjected Dow Jones to the jurisdiction of the British courts. See *Harrods Ltd. v Dow Jones & Co., Inc.* (2003) EWHC 1162 (QB), available online at http://www.courtservice.gov.uk/judgmentsfiles/j1769/harrods_v_dow_jones.htm. The case began with an April Fools press release suggesting that Harrods was contemplating a public offering of its shares. The Wall Street Journal reported on the joke press release and suggested that, "If Harrods, the British luxury retailer, ever goes public, investors would be wise to question its every disclosure." *Harrods, Ltd. v Dow Jones & Co., supra.* Harrods responded by suing Dow Jones for libel in London. The court reasoned that "however limited and technical" they may be, English publications about an English corporation "are most conveniently dealt with in an English court." *Harrods, Ltd. v Dow Jones & Co., supra.*

Later, Dow Jones petitioned a U.S. federal district court to exercise jurisdiction over the case in the United States, but the court declined. *Dow Jones & Co. v Harrods, Ltd*. (SD NY 2002) 237 F Supp 2d 394, aff'd (2d Cir 2003) 346 F3d 357. Although the Second Circuit opinion affirming the district court's decision was limited to a discussion of grounds under the Declaratory Judgment Act (346 F3d at 359), the district court's analysis of its interest in upholding principles of international comity is nonetheless instructive. See 237 F Supp 2d at 443.

In *Bangoura v Washington Post Co.* (Ontario Ct App, Sept. 16, 2005, C41379) (see http://www.ontariocourts.on.ca/decisions/2005/september/C41379.htm), a Canadian appeals court reversed a controversial lower court decision in an Internet libel action involving articles published in the Washington Post and made available online. The lower court relied heavily on *Gutnick*'s reasoning, rejecting jurisdictional challenges and holding that the case could be brought in Canada. The plaintiff was a former U.N. official who did not reside in Ontario at the time of publication. Finding that the newspaper had seven paid subscribers in Ontario and that the articles in question had been downloaded only one time, by the plaintiff's counsel, the court held that the action had no "real and substantial connection" to Ontario. The case garnered intense international interest, with a coalition of over 40 media organizations and advocacy groups intervening following the trial court ruling.

In *Yousef Jameel v Dow Jones & Co., Inc.* (2005) EWCA Civ 75, the English Court of Appeal reversed the lower court and dismissed a libel action brought in London by a Saudi businessman based on publication of an article by the Wall Street Journal on its Internet site. The article listed an individual whose name was similar to the plaintiff's name and who was alleged to have contributed money to the al Qaeda terrorist organization. In facts similar to *Bangoura*, only five subscribers had actually accessed the article; the court found that there was only minimal publication and minimal damage to the plaintiff's reputation in England. But see *King v Burstein* (2004) EWCA Civ 1329, in which the English Court of Appeal upheld Don King's libel action in England based on statements made and quoted on U.K. sports-related Internet sites. The court cited *Gutnick* and deferred to the discretion of the trial court in evaluating the appropriateness of the English forum. See http://www.hmcourts-service.gov.uk/judgmentsfiles/j2261/king-v-lewis.htm.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/21 International Issues/§21.5 E. Comity: Enforcing Foreign Judgments Against U.S. Companies

§21.5 E. Comity: Enforcing Foreign Judgments Against U.S. Companies

Under general principles of international comity, the judgment of a foreign court is conclusive in a federal court of the United States when (*International Transactions, Ltd. v Embotelladora Agral Regiomontana, SA de CV* (5th Cir 2003) 347 F3d 589, 594):

> (1) the foreign judgment was rendered by a court of competent jurisdiction, which had jurisdiction over the cause and the parties, (2) the judgment is supported by due allegations and proof, (3) the relevant parties had an opportunity to be heard, (4) the foreign court follows procedural rules, and (5) the foreign proceedings are stated in a clear and formal record.

The doctrine of comity is not unrestricted, however. Under Restatement (Third) of Foreign Relations Law of the United States §482, as adopted by the Third Circuit in U.S. v Small (3d Cir 2003) 333 F3d 425, 428, rev'd on other grounds (2005) 541 US 385, there are two mandatory and six discretionary grounds for a United States court to refuse to recognize a foreign judgment: A U.S. court may not recognize a judgment of a foreign court if:

- The judgment was rendered under a judicial system that does not provide impartial tribunals or procedures compatible with due process of law; or
- The court that rendered the judgment did not have jurisdiction over the defendant in accordance with the law of the rendering state.

A U.S. court need not recognize a judgment of a foreign court if:

- The court that rendered the judgment did not have jurisdiction of the subject matter of the action;
- The defendant did not receive notice of the proceedings in sufficient time to enable him to defend;
- The judgment was obtained by fraud;
- The cause of action on which the judgment was based, or the judgment itself, is repugnant to the public policy of the United States or of the State where recognition is sought;
- The judgment conflicts with another final judgment that is entitled to recognition; or
- The proceeding in the foreign court was contrary to an agreement between the parties to submit the controversy on which the judgment is based to another forum.

See Restatement (Third) of Foreign Relations Law of the United States §482.

The limits of the doctrine of comity have been and continue to be addressed in a series of decisions involving Yahoo! and its online auction site. See *Yahoo!, Inc. v La Ligue Contre le Racisme et L'Antisemitisme* (ND Cal 2001) 169 F Supp 2d 1181, rev'd and remanded with instructions to dismiss without prejudice (9th Cir 2006) 433 F3d 1199. Yahoo! was found liable by a French court under French law for offering Nazi memorabilia for sale on its auction site, and was ordered to block French citizens' access to its offending website. Yahoo! subsequently sought declaratory relief in the United States that the French order was not enforceable in the United States. The district court agreed with Yahoo! that a French tribunal did not have jurisdiction over an American company merely by way of its website, holding that the French court's order was "neither cognizable nor enforceable under United States law." 169 F Supp 2d at 1186. The court stated that, absent a body of law specific to Internet speech regulation, "the principle of comity is outweighed by the Court's obligation to uphold the First Amendment." 169 F Supp 2d at 1192.

On appeal, the Ninth Circuit initially reversed, rejecting the district court's conclusion that it could exercise specific jurisdiction over the French appellants. Instead, the appeals court held that, because the district court lacked general jurisdiction, specific jurisdiction would require a showing of "express aiming" at the forum state by the French appellants. "[F]or [the French appellants'] litigation efforts against Yahoo! to amount to 'express aiming,' those efforts must qualify as wrongful conduct targeted at Yahoo!" *Yahoo!, Inc. v La Ligue Contre le Racisme et L'Antisemitisme* (9th Cir 2004) 379 F3d 1120, 1125. The court did not find the requisite wrongful conduct. After its initial reversal, however, the Ninth Circuit voted to rehear the case en banc. *Yahoo!, Inc. v La Ligue Contre le Racisme et L'Antisemitisme* (9th Cir 2005) 399 F3d 1010. Yahoo! subsequently prohibited the sale of Nazi memorabilia on its auction sites worldwide

and implemented other restrictions on access to similar material.

Early in 2006, the Ninth Circuit en banc panel dismissed the case without prejudice, holding that although the French parties had sufficient contacts with California to be subject to personal jurisdiction in the state, the dispute was not ripe. *Yahoo!, Inc. v La Ligue Contre le Racisme et L'Antisemitisme* (9th Cir 2006) 433 F3d 1199. The orders issued by the French court were expressly aimed at California, the court held, and resulted in "significant acts" there, including required changes to Yahoo!'s servers, located in California, and the fact that the impact of a penalty imposed by the French court's orders would affect Yahoo! at its California headquarters. The court found, however, that Yahoo!'s change of policy, which brought it partially into compliance with the French court's orders, mooted the dispute, bringing Yahoo!'s suit "perilously close to a request for a forbidden advisory opinion." 433 F3d at 1223.

A U.S. entity may be more vulnerable to judgments in jurisdictions where it maintains a physical presence, including personnel, or assets with which to satisfy a local judgment. See *Ex-CompuServe Boss Acquitted*, BBC Online Network (Nov. 17, 1999), available at http://news.bbc.co.uk/1/hi/world/europe/524951.stm (in Germany, lower court's decision holding ISP's local manager liable for ISP's distribution of pornography, over which manager had no control, was overturned).

© The Regents of the University of California

§21.6 F. Content Filtering by Foreign Governments

Certain foreign governments attempt to enforce cultural or legal prohibitions through content filtering on the Internet. China in particular is known for its policy of filtering websites for speech critical of the Chinese government and otherwise trying to control the Internet access of its citizens. See generally *Internet Filtering in China,* OpenNet Initiative (June 15, 2009), available at http://opennet.net/research/profiles/china. Other countries have cited religious values to justify widespread blocking of Internet websites, including many websites that otherwise enjoy worldwide popularity. See, *e.g.,* Saudi Internet Rules, available at http://www.al-bab.com/media/docs/saudi.htm. OpenNet Initiative publishes current global Internet filtering maps at http://map.opennet.net.

Some companies doing business online choose to ignore restrictive national policies, particularly if the business has no physical presence in the country that prohibits the content or product offered. Other companies have undertaken self-regulation or self-censorship with respect to particular content in the interests of discouraging more aggressive attempts by foreign governments to regulate e-commerce. Others have chosen to filter content viewable in local markets based on local laws and sensitivities. See, *e.g.,* McCullagh, *No Booze or Jokes for Googlers in China*, CNET News.com (Jan. 26, 2006), available at http://news.cnet.com/2100-1030_3-6031727.html.

In a ruling interpreting the EU Information Society Directive (the Copyright Directive) 2001/29/EC, a Belgian court ordered a Belgian ISP to install filtering technology to prevent its customers from illegally sharing music and video files. See Niccolai, *Court Holds Belgian ISP Responsible for File-Sharing* (July 5, 2007), available at http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9026360.

© The Regents of the University of California

§21.7 G. How to Target or Not Target Certain Countries

Although the reach of the Internet is global, conforming a website to the legal and cultural requirements of specific foreign countries may help online businesses avoid criminal prosecution or civil litigation abroad. Certain measures can help discourage or eliminate interaction with residents of countries where a website's content or product may face legal challenges. The following steps can be useful in limiting the geographical scope of the markets intended to be targeted by a company's website:

- Direct website visitors to a dropdown list that includes only the names of countries intended to be targeted by the website.
- Place a conspicuous notice on the website informing site visitors that if they are citizens of named countries, the laws of their countries prohibit them from accessing or using the website.
- Avoid accepting orders of goods from, or shipping orders to, countries where commerce in the goods is prohibited.
- Consider implementing a registration process that requires address information from website users, which can be used to exclude users attempting to access the website from prohibited territories.

Filtering content based on geopolitical boundaries, or "geo-filtering," to the extent technology allows, is another way to minimize the risk of liability in countries where specific content or goods are prohibited. To the dismay of proponents of a truly global Internet, software has been developed that blocks an end user's access by associating the computer's Internet address with a particular nation. Geo-filtering software successfully identifies the home country of an Internet address 98 percent of the time, although determined users are attempting to keep pace with it by developing ways to hide their locations. See Cha, *Rise of Internet "Borders" Prompts Fears for Web's Future*, Washington Post (Jan. 4, 2002).

© The Regents of the University of California

§21.8 H. International Electronic Contracting

Contracts formed in cyberspace, like those formed in traditional international paper transactions, may be undermined by inconsistent laws governing contract formation in the relevant jurisdictions. The United Nations Commission on International Trade Law (UNCITRAL) adopted the Convention on the Use of Electronic Communications in International Contracting, which is intended to remove obstacles to the use of electronic communications in international contracting and to enhance legal certainty and commercial predictability. In general, these rules are intended to parallel those that apply to contracting on paper and to assure contracting parties that contracts negotiated electronically are as valid and enforceable as traditional paper-based transactions. The text of the Convention is available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html.

© The Regents of the University of California

§21.9 I. International Intellectual Property Protection

The World Intellectual Property Organization (WIPO), based in Geneva, Switzerland, is an agency of the United Nations whose primary purpose is to protect intellectual property through administration of international treaties and resolution of cross-border disputes for businesses. WIPO provides alternative dispute resolution services for businesses, with a focus on resolving patent, trademark, and domain name disputes. See §§3.14, 3.17, 3.18. In an effort to promote the importance of careful contract drafting to avoid litigation, WIPO also provides model contract clauses setting forth the requirement that disputes between contracting parties be submitted to WIPO for mediation or arbitration. See http://www.wipo.int/amc/en/index.html.

In addition to WIPO's programs, the European Union copyright directive (2001/29/EC) contains many provisions reflecting the Copyright Treaty and the Performances and Phonograms Treaty adopted previously by WIPO. See http://www.wipo.int/treaties/en/ip/wct (WIPO Copyright Treaty), http://www.wipo.int/treaties/en/ip/wppt (WIPO Performances and Phonograms Treaty), and http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:167:0010:0019:en:pdf (EU Copyright Directive). The directive also contains anti-circumvention provisions similar to those in the Digital Millennium Copyright Act. See §§1.25-1.26.

© The Regents of the University of California

J. European Union Directives

§21.10 1. Introduction

Like treaties, European Union directives represent a multinational approach to regulating transborder policies and practices. The directives set minimum standards for legislation on matters of common concern to EU member states, including commerce. Counsel to American companies doing business online should keep in mind that individual member states are free to enact more aggressive legislation to protect citizens in consumer transactions. Although most directives set parameters for policies and practices within the European Union, some explicitly set standards for nonmember businesses dealing with EU citizens. Even commerce-oriented directives that do not expressly address extraterritorial businesses, however, may be viewed as guidelines for business-to-business and business-to-consumer transaction with citizens of the European Union.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/21 International Issues/ 2. EU Data Protection Directive/ §21.11 a. Generally

2. EU Data Protection Directive

§21.11 a. Generally

The European Union Data Protection Directive (EU Directive 95/46/EC) is a model for data protection and privacy legislation among the EU member states. The directive prohibits the transfer of personal data concerning European citizens to any countries outside Europe that lack "adequate protection" standards for safeguarding the privacy of personal data. On EU data protection directives, see http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm. The directive is intended to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data," and requires application of the following principles:

- Personal data should be collected only for specified, legitimate purposes;
- Individuals should be informed about the purposes for data collection and the identity of the entity controlling the data;
- Each individual should have a right of access to his or her data and the opportunity to change or delete incorrect data; and
- In the event of any misuse of data, appropriate remedies must be available.

In 2002, the EU passed a directive intended in part to harmonize the regulations passed by member states in order to comply with the 1995 directive. EU Directive 2002/58/EC. France has yet to adopt any version of the directive, although France has had similar, preexisting data protection laws in place. Fortunately, U.S. companies that wish to do business with EU customers, or companies or that might have a need to transfer data to or from EU member nations, can choose from two relatively simple means for compliance with the EU data protection directive: (1) registration under the EU-U.S. safe harbor agreement or (2) case-by-case, contract-based compliance.

The Article 29 Working Party, a committee of Europe's data protection regulators, has issued an opinion advising social networking sites (defined as "online communication platforms which enable individuals to join or create networks of like-minded users") that they must comply with the EU Data Protection Directive if they handle personal data of EU residents. Such sites cannot avoid legal obligations using the argument that they are located outside the EU. Social networking sites, providers of third party applications that interact with these sites, and, in some cases, users may have to comply with consent requirements for the sharing of common material found on such sites, such as pictures, statements of political opinions, and information about users' health and sex lives. See http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/21 International Issues/ b. Compliance With EU Data Protection Directive/§21.12 (1) Safe Harbor Certification

b. Compliance With EU Data Protection Directive

§21.12 (1) Safe Harbor Certification

For companies that would prefer not to pursue compliance with the EU directive on a case-by-case basis, an agreement reached in 2000 between the European Commission and the U.S. Department of Commerce offers an alternative: "Safe Harbor" certification. To be eligible for safe harbor protection, a company must agree to comply with seven data protection principles, essentially designed to mirror the principles of the EU directive in important respects. See http://www.export.gov/safeharbor/index.asp. The safe harbor principles—notice, choice, onward transfer, access, security, data integrity, and enforcement—include the following requirements:

- Clear and conspicuous notice of data collection practices;
- The ability for individuals to opt out of data collection (and, for certain sensitive data, a requirement that individuals instead affirmatively opt in for certain uses of that data);
- Maintenance of security precautions;
- Enforcement mechanisms for individuals with complaints or disputes concerning data collection; and
- Individual access to the information maintained about them.

In the EU data protection regime, EU regulators are empowered to commence legal proceedings against companies that violate the data protection regulations. Companies that obtain safe harbor certification will be deemed to have adequate protection sufficient to comply with the regulations, and can operate with some assurance that their data transfer and use will not be interrupted.

PRACTICE TIP: Although safe harbor certification can be requested through an online application process, critics have questioned whether certification offers any benefits. See McCullagh, *Safe Harbor Is a Lonely Harbor,* Wired News (Jan. 5, 2001), http://www.wired.com/news/politics/0,1283,41004,00.html. Until safe harbor certification gains wider acceptance—which may require greater conformity of privacy laws among EU member states and between the EU and the U.S.—companies may be better served by pursing compliance with the data protection directive on a case-by-case basis, or by taking steps to ensure that their business operations do not trigger any obligations under the directive.

Safe harbor certification requires annual self-certification to the FTC. See http://www.export.gov/safeharbor/eu/eg_main_018476.asp. Failure to do so may result in FTC action. In 2009, for example, six companies (World Innovators, Inc.; ExpatEdge Partners, LLC; Onyx Graphics, Inc.; Directors Desk LLC; Collectify LLC; and Progressive Gaitways, LLC) agreed to settle FTC charges of unfair and deceptive business practices for representing that they held current certifications to the safe harbor program even though they had allowed their certifications to lapse. See the FTC press release, *FTC Settles With Six Companies Claiming to Comply With International Privacy Framework* (Oct. 6, 2009), at http://www.ftc.gov/opa/2009/10/safeharbor.shtm.

The EU Data Protection Directive, while generally recognized as an effort to protect privacy rights, has raised concerns in the United States regarding the possible targeting of U.S.-based multinational corporations by EU member states in the enforcement of legislation enacted under the directive. Indeed, some U.S.-based companies (and EU companies with operations in the United States) have already been accused of not complying with a particular EU member state's version of the directive. See, *e.g.,* Watson, *Amazon Case Triggers Data Protection Confusion* (Dec. 15, 2000), available at http://management.silicon.com/government/0,39024677,11021592,00.htm.

As described in §21.13, one way for companies to comply with the directive is to obtain individual consent to data collection, use, and transfer. Often, a contractual consent provision can prove an effective way to avoid violating any European privacy or data protection regulations.

PRACTICE TIP: Information on the EU data protection directives is maintained on the Web at http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm. Additional information on Internet initiatives regarding

privacy, safety, and human dignity throughout the EU and its member states is available at http://www.saferinternet.org.

© The Regents of the University of California

§21.13 (2) Case-by-Case Compliance; Model Contract Clauses

As an alternative to safe harbor certification, companies doing business online can pursue compliance with the EU Data Protection Directive on a case-by-case basis, by relying on contract language intended to ensure that the parties will use and transfer data only in ways that will not run afoul of EU regulations. Under one exemption to the EU directive, data can be transferred with the consent of the individual who is the subject of the data. See Article 7(a), Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, accessible from http://ec.europa.eu/justice_home/fsj/privacy. As a result, any opportunity to form a binding agreement with an individual who will be asked to provide data, such as an end-user license agreement or other website user agreement, is an opportunity to obtain that individual's consent to the transfer of data. For a discussion of online agreements and their enforceability, see chap 8.

The European Commission has adopted measures setting out model contract clauses designed to ensure appropriate safeguards for transfers of data from EU member states to countries outside the EU. These clauses are intended to offer an alternative way to obtain sufficient "adequate protection" (see §21.11) to protect the flow of data from EU member states from interruption. See http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/21 International Issues/ 3. Other EU Directives/§21.14 a. Distance Selling

3. Other EU Directives

§21.14 a. Distance Selling

The EU Directive on Protection of Consumers in Respect to Distance Contracts (97/7/EC) (see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0007:EN:HTML) applies to any business that enters into a contract with an EU consumer. The directive requires that consumers be provided with information on the identity of the seller as well as a means to contact the seller. In addition, the directive requires that the following information be addressed:

- The main characteristics of the goods or services;
- The price, including taxes and delivery costs;
- After-sale services and guarantees;
- Where to send complaints; and
- The right of withdrawal from the contract.

The directive also prohibits demands for payment in cases of "inertia selling," *i.e.,* the practice of supplying a consumer with unsolicited goods, or considering the absence of a response as equivalent to an affirmative order. EU consumers may not waive their rights under the directive.

© The Regents of the University of California

§21.15 b. E-Commerce Directives

The European Union issued a directive in 2000 addressing "information society services," which encompass a broad range of activities that take place online. See EU Directive 2000/31/EC at http://ec.europa.eu/internal_market/e-commerce/directive_en.htm. Although the directive was intended to set forth principles governing EU countries, non-EU businesses offering services to EU customers should be familiar with its provisions. The directive requires member states to recognize electronic contracts, and limit liability of a service provider acting as a "mere conduit." The directive also addresses advertising and direct marketing, requiring member-states to ensure that any commercial communications is "identifiable clearly and unambiguously as such as soon as it is received" and that service providers regularly consult opt-out lists.

One example of some of the nuances applicable to Internet businesses operating in the EU relates to support and other service inquiries. Article 5, §1 of the E-Commerce Directive requires service providers to provide contact information to recipients of their services. In *Bundesverband der Verbraucherzentralen und Verbraucherverbände-Verbraucherzentrale Bundesverband eV v deutsche internet versicherung AG* (Case C-298/07), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62007J0298:EN:HTML, the European Court of Justice ruled that merely posting an e-mail address for contact purposes is not sufficient. To comply with the directive, the site must provide "other information which allows the service provider to be contacted rapidly and communicated with in a direct and effective manner." The court clarified that the site does not necessarily have to post a telephone number. Alternatively, the site can provide

> an electronic enquiry template through which the recipients of the service can contact the service provider via the [I]nternet, to whom the service provider replies by electronic mail except in situations where a recipient of the service, who, after contacting the service provider electronically, finds himself without access to the electronic network, requests the latter to provide access to another, non-electronic, means of communication.

© The Regents of the University of California

§21.16 c. VAT Directive

In an effort to level the e-commerce playing field, the European Union now requires non-EU vendors of digital products to charge Value Added Taxes (VAT) on Internet sales to EU consumers. EU Directive 2002/38/EC. See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0038:EN:HTML. The directive also eliminates the burden of collecting VAT from EU vendors selling digital products to non-EU customers.

© The Regents of the University of California

§21.17 d. Specific Industry Directives

In order to sell certain products to European Union customers, manufacturers must provide proof of conformity with minimum safety requirements through CE marking (from the French "Conformité Européenne"), documentation that indicates the product meets the requirements set forth in the relevant EU directive. CE marking does not guarantee the safety or quality of the product, and usually does not require outside testing, but simply provides an indication that the product's manufacturer has met its legal requirements, and the product may therefore be distributed in EU member states. A complete list of EU directives governing products that require CE marking, including gas appliances, certain medical devices, toys, and electromagnetic devices, is available on the Web at http://ec.europa.eu/enterprise/policies/european-standards/documents/harmonised-standards-legislation/list-references/.

NOTE: China, too, in the interest of quality control, requires many imported manufactured products to bear the China Compulsory Certification (CCC) mark. See, *e.g.,* http://219.238.178.8/20040420/column/227.htm. Other nations requiring product certification marks include New Zealand, Korea, Japan, Australia, and India. See, *e.g.,* http://www.nata.asn.au (Australia); http://www.jab.or.jp/english/index.html (Japan).

© The Regents of the University of California

§21.18 e. EU Privacy Directive

The European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, No. 95/46/EC (Oct. 24, 1995), also known as the EU Privacy Directive, applies to collection, transfer, and use of information collected from websites. The EU Privacy Directive and a safe harbor negotiated by the United States Department of Commerce are discussed in §§9.37-9.38. See amendments to the EU Privacy Directive regarding the use of "cookies," or similar tracking technologies, available at http://register.consilium.europa.eu/pdf/en/09/st03/st03674-re01.en09.pdf.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/21 International Issues/§21.18A f. EU Data Retention Directive

§21.18A f. EU Data Retention Directive

The EU Directive on Data Retention (2006/24/EC) requires all telephone and Internet traffic to be logged and stored for between 6 months and 2 years in order to help combat organized crime and terrorism. Telephone companies must keep data on the time of each land line and cell phone call made in Europe, whether the call is answered, the length of the call, and other details to assist in tracing the caller. ISPs will be required to retain data on IP addresses and Internet connections, and data to assist in tracing e-mails and Voice over Internet Protocol (VoIP) calls. Reimbursement of costs to telephone service providers and ISPs will be the responsibility of each member state. For the complete text of the directive, see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML.

© The Regents of the University of California

K. Self-Regulation

§21.19 1. Trustmarks

In the interest of limiting government regulation and fostering consumer trust in e-commerce, international business and consumer organizations are exploring ways to promote self-regulation of online businesses. One method already practiced on a national scale in the United States is website certification, which assures consumers that the site they are visiting adheres to certain business standards. Certification is indicated by a "trustmark"—a seal or banner displayed on the web pages of subscribing businesses.

For example, an online business with a physical presence in the United States or Canada may apply for privacy or reliability seals offered by the Better Business Bureau. See http://www.bbbonline.org. Applicants for the Better Business Bureau privacy seal must pay a fee and sign the organization's extensive online Privacy Participation Agreement, which covers privacy notice requirements, sharing of information, access to and correction of information, and security. To further qualify to display the seal, an applicant must adopt and post a privacy notice and assign a specific individual responsibility for implementing and overseeing the policy. Businesses whose privacy policies are limited to certain countries must agree not to transact business in countries whose residents are not protected by their policies. A specialized program is available to businesses whose services are directed to children under 13.

The Global Trustmark Alliance, an international group of trustmark organizations, has undertaken an effort, supported by a 3-year, $400,000 grant from the U.S. Department of Commerce, to establish a single, globally recognized trustmark. See BBB*Online* Update (June 2002), at http://www.bbbonline.org/update/issue.asp?ID=29#237 (describing formation of Global Trustmark Alliance). Numerous organizations and businesses offer site certification and related services, including TRUSTe (http://www.truste.org), established by a nonprofit group; WebTrust (http://www.webtrust.org), a project of the American Institute of Certified Public Accountants; and VeriSign (http://www.verisign.com) and GeoTrust (http://www.geotrust.com), for-profit providers of Internet certification and security services worldwide.

© The Regents of the University of California

§21.20 2. International ADR

Given the volume of international business transactions conducted online and the conflicts inherent in international litigation, governments and international businesses are exploring ways to promote alternative methods of resolving business-consumer disputes. Trustmark providers require subscribers to agree to alternative dispute resolution, and the European Union's directive on e-commerce (see §21.15) calls on member states to avoid adopting regulations that could discourage out-of-court dispute settlements. ADR proponents favor access—possibly online—to impartial, inexpensive, and expeditious alternatives to judicial proceedings for dispute resolution.

Government, private organizations, and businesses—including the International Chamber of Commerce (http://www.iccwbo.org), the American Arbitration Association (http://www.adr.org), and the World Intellectual Property Organization (WIPO) (http://www.wipo.int)—have made various proposals for ADR relating to e-commerce transactions. For a discussion of alternatives to judicial resolution of international e-commerce disputes, including mediation and the use of credit card chargebacks, see *Note*, Hastings Int'l & Comp L Rev 383 (Summer 2002).

© The Regents of the University of California

II. EXPORT CONTROLS ON COMMERCIAL SOFTWARE AND TECHNOLOGY

§21.21 A. Introduction

United States export controls cover the transmission of U.S.-origin items, such as software and technical data. They also cover the transmission of items out of the United States, regardless of their origin, *e.g.,* sending an e-mail or making information available for download on a website. Anyone doing business on the Internet should be aware of export controls and how to comply with them.

The United States imposes export controls so that it can regulate and control the extent to which certain know-how is shared abroad. Export controls have assumed heightened importance in the last several years because of concerns over national security. U.S. export controls are administered principally by three federal agencies: (1) the U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC), which administers export controls on transactions with sanctioned or embargoed nations; (2) the U.S. Department of State, Directorate of Defense Trade Controls (DDTC), which administers export controls on military products and services; and (3) the U.S. Department of Commerce, Bureau of Industry and Security (BIS), which administers export controls on commercial products and technology. (The BIS website, at http://www.bis.doc.gov, offers helpful information for exporters.) Sections 21.2-21.48 briefly review U.S. export controls on commercial products and technology administered by BIS under the Export Administration Regulations (EAR) (15 CFR pts 730-774). These controls exist because, although the affected products are commercial in nature, they are considered to have the potential for "dual use," *i.e.,* concurrent military or strategic applications. 15 CFR §730.3. The EAR provides a list of "items" (*i.e.,* commodity, software, technology) to which commercial export controls apply, known as the "Commerce Control List" (CCL), at 15 CFR pt 774, Supp No. 1. See §21.27. If an item is subject to U.S. export controls, it means an export license may be required and that certain restrictions may apply on where it may be exported, to whom it may be exported, and for what purpose it may be exported.

Export control issues can arise in many types of software transactions. For example, they arise if a United States company is jointly developing software with one or more parties outside the United States, such as by outsourcing some of the code development to programmers at an offshore facility. They arise in the license and distribution agreements the company may enter into with U.S. and foreign distributors, who may reexport the software. Finally, they arise with respect to the company's software sales.

United States persons are responsible for complying with U.S. export controls, regardless of the conduct of any other parties to the transaction. Therefore, a U.S. company cannot simply "contract away" this responsibility when negotiating agreements with other parties. Sections 21.49-21.61 review compliance issues for managing a company's online export transactions.

WARNING: Export control regulations are exceedingly complex. Sections 21.2-21.48 provide an overview of export control analysis as applied to commercial export of software, but practitioners should always consult the EAR directly when advising a client regarding specific transactions. Practitioners unfamiliar with export transactions should consult an experienced international lawyer.

© The Regents of the University of California

§21.22 B. Export Control Analysis

Export control analysis involves five questions: (1) what is the transaction; (2) what is the product; (3) who is the recipient of the product; (4) for what purpose will the product be used; and (5) what actions are necessary to comply with the regulations. See http://www.bis.doc.gov/licensing/exportingbasics.htm.

© The Regents of the University of California

§21.23 1. Transactions Subject to Export Controls

The first step is to determine whether the proposed transaction is covered by export controls. Any "item" (*i.e.,* commodity, software, technology) *in* the United States may be subject to the Export Administration Regulations (EAR). 15 CFR §734.3(a)(1). Any U.S.-origin item on the "Commerce Control List" (CCL) (see §21.27) may be subject to the EAR, even if it is *outside* the United States. 15 CFR §734.3(a)(2). Even certain items not specifically identified on the CCL may be subject to the EAR, unless they are publicly available. 15 CFR §734.3(b)(3), (c). A foreign-origin item may also be subject to the EAR if it contains a threshold amount of "U.S. content," or if it is exported or reexported from the United States. See 15 CFR §734.3(a)(3).

© The Regents of the University of California

§21.24 2. Definition of "Export"

The common notion of an export is a physical shipment of tangible merchandise out of the United States to a foreign country. For export control purposes, however, the definition of "export" is much broader. Under the EAR, an export is defined as follows (15 CFR §734.2(b)(1)):

> "Export" means an actual shipment or transmission of items subject to the EAR out of the United States, or release of technology or software subject to the EAR to a foreign national in the United States.

Because an export includes a "transmission" of items out of the United States, it could include sending an e-mail or making information available for download on a website. See, *e.g.,* 15 CFR §734.2(b)(9)(i)(A). Thus, the term "export" would include an engineer e-mailing technical specifications concerning the company's software to an offshore programming facility in India, or a sales representative instructing a customer in Singapore on how to download encryption software from the company's website.

In addition, an export includes a "release" of technology. This could include providing technical information or assistance, even informally. See 15 CFR §734.2(b)(2)(i), (b)(3). For example, it could include a developer's explanation of how to change a software program's encryption to officials of a Spanish company meeting at a trade show in Chile.

An export also includes a release of software (in source code) or technology to a foreign national, even if the foreign national is located within the United States. 15 CFR §734.2(b)(2)(ii). This could include making the item or information available for visual inspection by foreign nationals, orally exchanging information, or applying abroad technical experience acquired in the United States. 15 CFR §734.2(b)(3). For example, it could include a company manager training an employee, who is a foreign national of China, on how to debug the software at the company's headquarters in California. Because a "foreign national" is an individual who is neither a U.S. citizen nor a U.S. lawful permanent resident (*i.e.,* green card holder), such a transaction is deemed an export because it is considered to be the same as actually exporting that item or information to the foreign national's country. 15 CFR §734.2(b)(2)(ii).

© The Regents of the University of California

§21.25 3. Fines and Penalties for Violations

Violations of the EAR are punishable with severe sanctions, including civil and criminal penalties. Companies may be fined up to the greater of $1 million or five times the value of the exports for each violation. 15 CFR §764.3(b)(2)(i). Individuals may be fined up to $1 million or imprisoned for up to 20 years for each willful violation. 50 USC §1705(c); 15 USC §764.3(b)(1)-(2). In addition, any violation of the EAR may also result in the imposition of a civil penalty of up to $250,000 for each violation, as well as the suspension or revocation of the authority to export goods or technology from the United States or to receive or participate in an export from the United States. 15 CFR §§6.4(a)(6)-(7), 764.3(a)(1)(i), (a)(2). Note that, because the Export Administration Act expired in 2001, the provisions above have continued in effect under the International Emergency Economic Powers Act (IEEPA) (50 USC §§1701-1707), as amended by the International Emergency Economic Powers Enhancement Act (Pub L 110-96, 121 Stat 1011).

© The Regents of the University of California

§21.26 C. Product Classification

If the company will be engaged in an export transaction, the company will first need to identify how the product is classified for export control purposes.

© The Regents of the University of California

§21.27 1. Commerce Control List (CCL); Export Control Classification Number (ECCN)

The Commerce Control List (CCL) (15 CFR pt 774, Supp No. 1) is a comprehensive listing and description of categories of items subject to export controls. Of its ten categories, the three categories usually most relevant to software companies are: Category 3: Electronics; Category 4: Computers; and Category 5: Telecommunications and Information Security (encryption capability). See 15 CFR §738.2(a). Each category is divided into groups, and each group comprises individual types of products identified by an alphanumeric code called an Export Control Classification Number (ECCN). See 15 CFR §738.2(d). Even if a product does not fall under a specific ECCN, it will still be subject to the EAR if it is classified as EAR99, which is a general designation on the CCL. 15 CFR §§734.3(c), 732.3(d)(5). The export control restrictions applicable to these classifications are reviewed in §§21.29-21.48.

© The Regents of the University of California

§21.28 2. Country Chart

Included in the Commerce Control List (CCL) (see §21.27) is a Country Chart that indicates the controls applied to different countries. If the Export Control Classification Number (ECCN) listing (see §21.27) identifies a reason for control that matches one marked for the particular country of export, it means the export of that product to that country would require a license, unless a license exception applies. The Country Chart is located at 15 CFR pt 738, Supp No. 1. Generally, the level of control for each ECCN depends on the ultimate destination to which it will be exported. For example, antiterrorism export controls apply only with respect to five countries (Cuba, Iran, North Korea, Sudan, and Syria), but national security export controls can apply with respect to several other countries. See §§21.40-21.42. The more "reasons for control" that apply to an item, the greater the likelihood that its export will require a license.

© The Regents of the University of California

3. Software Without Encryption

§21.29 a. Publicly Available Software

For software without encryption, the first question to ask is whether it is publicly available. "Publicly available" software is defined as that which (1) has already been or will be made generally available to the public by being published, including posting on the Internet; (2) arises during, or results from, certain fundamental research; (3) is released by instruction at academic institutions; or (4) is included in certain patent applications. 15 CFR §734.3(b)(3). Publicly available software is *not* subject to the EAR, although export controls administered by other agencies for other purposes may still apply (*e.g.,* embargoes). 15 CFR §734.3(b)(3).

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/21 International Issues/§21.30 b. Object Code or Source Code

§21.30 b. Object Code or Source Code

In the more likely event that the company is exporting proprietary software, the next question to ask is whether the software without encryption is in object code or source code. See 15 CFR §772.1. The EAR defines "object code" to be "[a]n equipment executable form of a convenient expression of one or more processes ('source code') that has been converted by a programming system," and "source code" to be "[a] convenient expression of one or more processes that may be turned by a programming system into equipment executable form ('object code')." 15 CFR §772.1. In short, software in object code is a program that can be directly executed by a computer, while software in source code provides the instructions for that program. If the software is in object code, it will likely be classified as EAR99 (see §21.27). If it is in source code, the next question to ask is whether it is for an application or for an operating system. If the source code is for an application, it will still likely be classified as EAR99. If the source code is for an operating system, however, it may be classified as ECCN 4D003, meaning "operating system software… designed for multi-data stream processing equipment, in source code." 15 CFR pt 774, Supp No. 1. An export license would be required to export such source code to countries for which national security and/or antiterrorism controls apply.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/21 International Issues/§21.31 c. Software Incorporated in Computer Hardware

§21.31 c. Software Incorporated in Computer Hardware

In some cases, software will be exported when incorporated into computer hardware. Although the export of computers is controlled for several countries, computers are usually eligible for an exception to the licensing requirement (see 15 CFR §740.7), under which computers not exceeding a specified processing speed may be exported without a license, except to Cuba, Iran, North Korea, Sudan, and Syria or foreign nationals of those countries. See 15 CFR §740.7(b)(2), (d)(2). Because of the general availability of this license exception for hardware, the classification and licensing requirements for the entire item will usually be determined by the software.

© The Regents of the University of California

§21.32 4. Software With Encryption

Software with encryption is subject to special export controls. Encryption refers to the process of encoding data, which is akin to scrambling. It includes software with resident encryption or decryption capability incorporated into the product, as well as software that calls on third party products with such capability, including third party products from open sources.

Encryption items generally can be divided into two groups: those that require review by BIS prior to export and those that are exempt from such review. Encryption software requiring review generally is that which encrypts or decrypts data or text for secure communications using a key length in excess of 56 binary digits (bits)—which is a measure of how many combinations of keys with an encryption algorithm would be required to obtain a readable text. Encryption software that generally limits the use of cryptography to authentication (such as passwords for access control) is exempt from review, as is software, the encryption functionality of which falls into another specific category that BIS has exempted from review. See 15 CFR pt 742, Supp No. 5. See §21.34.

© The Regents of the University of California

§21.33 a. "Limited" Encryption Software Requiring Prior Review

Generally, encryption items requiring review by BIS actually perform bulk encryption, *i.e.,* encryption of data or text that has a key length in excess of 56 bits for symmetric algorithms (or in excess of 512 bits for asymmetric algorithms or in excess of 112 bits for elliptic curve algorithms). For mass market items, however, a prior review is required if the key length is in excess of 64 bits for symmetric algorithms.

A "mass market" item is defined as one that is generally available to the public for sale from stock at retail selling points in over-the-counter, mail order, online, or telephone transactions. 15 CFR §742.15(b); 15 CFR pt 774, Supp No. 1, Category 5, Information Security, Cryptography Note 3. A mass market item is also one in which the cryptographic functionality cannot be easily changed by the user and that is designed for installation by the user without further substantial support by the supplier. 15 CFR pt 774, Supp No. 1, Category 5, Information Security, Cryptography Note 3. Examples of mass market items include (15 CFR §742.15(b)(5)):

- General purpose operating systems and desktop applications (*e.g.,* e-mail, certain web browsers, games, word processing, database, financial applications, and utilities) designed for use with computers classified as ECCN 4A994 or EAR99, laptops, or hand-held devices;
- Commodities and software for client Internet appliances and client wireless LAN devices;
- Home use networking commodities and software (*e.g.,* personal firewalls, cable modems for personal computers, and consumer set top boxes); and
- Portable or mobile civil telecommunications commodities and software (*e.g.,* personal data assistants (PDAs), radios, and cellular products).

© The Regents of the University of California

b. "Full" Encryption Software Exempted From Prior Review

§21.34 (1) Limited Cryptography

BIS considers limited cryptography items to be those with cryptographic functionality that does not allow for encryption of files or text except as related to authentication. Authentication concerns access control, such as protection of passwords, Personal Identification Numbers (PINs), or similar data to prevent unauthorized access. 15 CFR pt 774, Supp No. 1, Category 5, Technical Note 2. Such items may include "personalized smart cards," those that provide for digital signature, and those that permit execution of copy-protected software. 15 CFR pt 774, Supp No. 1, ECCN 5A002; 15 CFR §742.15(b)(3)(iii). The export of these types of encryption software is generally controlled only for antiterrorism purposes, *i.e.,* to countries considered to be terrorist-supporting. See 15 CFR pt 774, Supp No. 1, Category 5, Information Security, ECCN 5D992.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/21 International Issues/§21.34A (2) Ancillary Cryptography

§21.34A (2) Ancillary Cryptography

Another category of encryption items exempted from review consists of items using ancillary cryptography, which is:

> the incorporation or application of "cryptography" by items that are not primarily useful for computing (including the operation of "digital computers"), communications, networking (includes operation, administration, management and provisioning) or "information security."

15 CFR §772.1. Ancillary cryptography items include items that are specially designed and limited to the following:

- Piracy and theft prevention for software and music;
- Games and gaming;
- Household utilities and appliances;
- Printing, reproduction, imaging, and video recording or playback, but not videoconferencing;
- Business process modeling and automation (*e.g.,* supply chain management, inventory, scheduling, and delivery);
- Industrial, manufacturing, or mechanical systems (including robotics, other factory or heavy equipment, facilities systems controllers including fire alarms, and HVAC); and
- Automotive, aviation, and other transportation systems.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/21 International Issues/§21.34B (3) Other Wireless Encryption Items

§21.34B (3) Other Wireless Encryption Items

Also exempted from review are items otherwise without encryption capability but that incorporate components or software that provide short-range wireless encryption functions, such as "Bluetooth" and "Wi-Fi," limited to a nominal operating range not exceeding 100 meters. 15 CFR §§740.17(b)(4)(i), 742.15(b)(3)(i).

© The Regents of the University of California

§21.35 5. Classification Procedures

Although an exporter may attempt to "self-classify" an item under the EAR, only a formal BIS classification ruling is binding for export control purposes. 15 CFR §748.3(a). Depending on whether the product contains encryption, BIS may require formal classification before export, and BIS suggests that exporters submit encryption items for formal classification if the exporter is unsure of the classification. 15 CFR §742.15(b)(1). There are different procedures applicable to classification of products with and without encryption capability. See 15 CFR §742.15(b)(1); 15 CFR pt 742, Supp No. 6; 15 CFR §§748.3(b), 748.4; 15 CFR pt 748, Supp No. 1. Classification requests and accompanying documents must be filed electronically through the BIS Simplified Network Application Processing system (SNAP-R). 15 CFR §748.1(d). For guidance on filing a commodity classification request with the BIS, see http://www.bis.doc.gov/licensing/cclrequestguidance.html. All information in a request is kept confidential by BIS and will not be disclosed to the public or third parties. 15 CFR §748.1(c).

Depending on the encryption functionality and strength, exporters of encryption products with full encryption, including certain mass market items (see §21.33), may be required to submit a review notification regarding their products before export, or to submit their products for a one-time review before export under License Exception ENC (Encryption Commodities and Software). 15 CFR §§742.15(b), 740.17(b). Absent these provisions, exporters would be required in many cases to obtain a license to export these products because they are controlled for national security reasons. Compliance with these provisions, however, eliminates the license requirement.

Once a product is reviewed and authorized by BIS, it may be upgraded to an increased key length without further review, provided that the exporter submits the following to BIS:

- A certification that no change has been made other than to upgrade the key length for confidentiality or key exchange algorithms;
- The original Commodity Classification Automated Tracking System (CCATS) authorization number issued by BIS and the date of issuance; and
- The new key length.

15 CFR §740.17(e)(2).

Alternatively, if a change is made to the cryptographic functionality or to other technical characteristics affecting mass market eligibility, then a new product review is required. 15 CFR §742.15(b). Such changes would include, for example, performance enhancements to provide network infrastructure services, or customizations to end-user specifications. 15 CFR §742.15. Alternatively, a new product review is not required when the change to the previously reviewed encryption product involves bundling, patches, upgrades, or releases of a product, or even a name change to the encryption product. 15 CFR §742.15.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/21 International Issues/§21.36 D. Development, Distribution, and Sales

§21.36 D. Development, Distribution, and Sales

Once the product is classified, the next step is to determine whether an export license is required to provide the item to others. Most commercial software can be exported either outright without a license or after qualifying for a license exception.

© The Regents of the University of California

1. General Rules

§21.37 a. Software Without Encryption

Even if the Commerce Control List (CCL) (see §21.27) and Country Chart (see §21.28) do not require an export license, the Export Administration Regulations (EAR) (15 CFR pts 730-774) require a license to export to certain end users or for certain end uses (see §§21.52-21.53). To cover these situations, the EAR includes the classification EAR99. 15 CFR §732.3(d)(5). Although a product classified as EAR99 does not fall under a specific ECCN subject to country restrictions, it is still subject to end user and end use restrictions. 15 CFR §732.3(h)(1).

© The Regents of the University of California

§21.38 b. Software With Encryption

The rules noted in §21.37 apply to all software, but software with encryption is subject to certain additional rules, depending on whether the software is for internal company use only or will be transferred outside the company.

Software with either limited or full encryption may be exported to foreign subsidiaries of U.S. companies without prior notification or review by BIS. 15 CFR §§742.15(b)(3)(i), 740.17(b)(1). Providing encryption software in source code to foreign nationals working as contractors, interns, or employees of U.S. companies in the U.S. or their foreign subsidiaries is not deemed to be an export if the software is for internal company use. 15 CFR §740.17(a)(2). Software in object code does not trigger the deemed export rule.

All items produced or developed by U.S. subsidiaries (see §21.19), with items exported or reexported under that exemption, may require review and authorization before they can be sold or retransferred outside of the U.S. company. Note to 15 CFR §740.17(a)(2). This provision permits exports to subsidiaries of any U.S. company, not just from the U.S. parent to its own subsidiary.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/21 International Issues/§21.39 (1) U.S. Subsidiaries

§21.39 (1) U.S. Subsidiaries

The Export Administration Regulations (EAR) (15 CFR pts 730-774) define a "U.S. subsidiary" as a "foreign branch of a U.S. company," or a "foreign subsidiary or entity of a U.S. entity" in which (15 CFR §772.1):

- The U.S. entity beneficially owns or controls (directly or indirectly) 25 percent or more of the voting securities of the foreign subsidiary or entity, if no other person owns or controls (directly or indirectly) an equal or larger percentage;
- The foreign entity is operated by the U.S. entity under the provisions of an exclusive management contract;
- A majority of the members of the board of directors of the foreign subsidiary or entity also are members of the comparable governing body of the U.S. entity;
- The U.S. entity has the authority to appoint the majority of the members of the board of directors of the foreign subsidiary or entity; or
- The U.S. entity has the authority to appoint the chief operating officer of the foreign subsidiary or entity.

© The Regents of the University of California

§21.40 (2) "Prohibited" Countries

No encryption item may be exported to any end user (including a U.S. subsidiary) in Cuba, Iran, North Korea, Sudan, or Syria ("prohibited" countries). 15 CFR §740.17. These are the five countries for which exports are controlled for antiterrorism purposes and to which BIS generally adopts a "policy of denial" toward export license applications. See, *e.g.,* 15 CFR §746.1(a)(1). In addition, no encryption source code or technology may be exported to a national of any of these countries, wherever that person may be located. 15 CFR §740.17. Further, U.S. embargos administered by the U.S. Department of the Treasury Office of Foreign Assets Control (OFAC) completely prohibit any transactions with certain countries. 31 CFR pts 500-597. The list of countries for which the United States maintains an embargo may be accessed on the OFAC website at http://www.treas.gov/offices/enforcement/ofac.

© The Regents of the University of California

§21.41 (3) "Preferred" Countries

Software with limited encryption may be exported to both government and nongovernment end users in any nonprohibited country as long as it meets one of the criteria to be considered for classification as an item with only limited use of encryption. 15 CFR §742.15(b). Generally, depending on whether or not the key length exceeds 56 bits in the symmetric algorithm, software with full encryption may be exported to both government and nongovernment end users in Austria, Australia, Belgium, Bulgaria, Canada, the Czech Republic, Cyprus, Denmark, Estonia, Iceland, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Japan, Luxembourg, Malta, the Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, and the United Kingdom ("preferred" countries) after the information required for a review is registered with BIS. 15 CFR pt 740, Supp No. 3; 15 CFR §740.17(b)(1)(i). An application is "registered" with BIS when it is entered into BIS's electronic license processing system. 15 CFR §750.4(a)(2). Note that exports to Canada are not subject to the review requirements. 15 CFR §742.15(a)(1).

Encryption items may also be exported without prior review to "preferred" countries for internal development or production of new products by "private sector end-users" headquartered in those countries. "Private sector end-users" are those not acting on behalf of any foreign government or not wholly owned by, or otherwise controlled by or acting on behalf of, any foreign government. 15 CFR §740.17(a)(1).

© The Regents of the University of California

§21.42 (4) "Permitted" Countries

For all countries not listed in §21.40 or §21.41 ("permitted" countries), exports of encryption items are permitted, but not to the extent as to the preferred countries. Specifically, software with encryption may be exported to any permitted country 30 days after the review is registered with BIS, *i.e.,* there is a waiting period. However, there is no waiting period if the key lengths do not exceed 80 bits for symmetric algorithms, 1024 bits for asymmetric algorithms, and 160 bits for elliptic curve algorithms. 15 CFR §740.17(b)(3). Such software may not be exported to government end users in the permitted countries without an export license if it is identified on a specific list of items. 15 CFR §740.17(b)(2)(iii), (b)(3)(i). These items include network infrastructure software, and software (15 CFR §740.17(b)(2)(iii)):

- That has been designed, modified, adapted or customized for government end use, including encryption commodities and software for external security operations center (SOC)/network operations center (NOC) command and infrastructure, public safety radio, and digital forensics/computer forensics;
- For which the cryptographic functionality has been modified or customized to customer specification; or
- For which the cryptographic functionality or encryption component is user-accessible and can be easily changed by the user.

© The Regents of the University of California

§21.43 (5) "Retail" Encryption Items [Deleted]

This section has been deleted consistent with regulatory changes.

© The Regents of the University of California

§21.44 c. "Cryptanalytic" Items

"Cryptanalytic" items, which may be exported only to nongovernment end users (15 CFR §740.17(b)(2)(iv)), are defined as (15 CFR §772.1)

> systems, equipment, applications, specific electronic assemblies, modules and integrated circuits designed or modified to perform cryptanalytic functions, software having the characteristics of cryptanalytic hardware or performing cryptanalytic functions, or technology for the development, production or use of cryptanalytic commodities or software.

© The Regents of the University of California

2. Special Rules

§21.45 a. Beta Test Software

▶ To download **Word** version, right click and choose *Save Target As*

▶ To download **WordPerfect** version, right click and choose *Save Target As*

Beta test software may be exported under License Exception TMP (Temporary Exports), except to "prohibited" countries. 15 CFR §740.9(c)(2). See §21.20. For beta test software to be eligible for this license exception, the software producer must intend to market the software to the general public after completion of beta testing. 15 CFR §740.9(c)(4)(i). In addition, the software producer must provide the beta test software to the consignee free of charge (or at a price not exceeding the cost of reproduction and distribution), and the software must be designed for installation by the end user without further substantial support from the supplier. 15 CFR §740.9(c)(4)(ii)-(iii). For encryption beta test software, the producer must submit a questionnaire response to BIS by the time of export. 15 CFR §740.9(c)(8). Before exporting the software, the exporter must obtain the following statement from the tester (15 CFR §740.9(c)(5)):

We certify that this beta test software will only be used for beta testing purposes, and will not be rented, leased, sold, sublicensed, assigned, or otherwise transferred. Further, we certify that we will not transfer or export any product, process, or service that is the direct product of the beta test software.

All beta test software must be destroyed or returned to the exporter within 30 days of the end of the testing period. 15 CFR §740.9(c)(7).

© The Regents of the University of California

§21.46 b. Encryption Source Code

The rules for export of encryption source code vary depending on the source code's technical classification. See 15 CFR §§740.17(b)(2)(iii), 742.15(b). A review registered with BIS is required in certain cases. See 15 CFR §742.15(b)(1)(ii)(B). Encryption source code may not knowingly be exported to any of the "prohibited" countries. 15 CFR §740.13(e)(4). See §21.20.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/21 International Issues/§21.47 c. Publicly Available Source Code

§21.47 c. Publicly Available Source Code

Source code may be exported without BIS review if it is "publicly available," *e.g.,* posted on the Internet. See 15 CFR §734.3(b)(3); §21.9. Source code may still be considered publicly available even if it is subject to an express agreement for the payment of a licensing fee or royalty for commercial production or sale of any product developed using the source code. 15 CFR §740.13(e)(1). Before making source code publicly available, the exporter must provide BIS with either a copy of the source code or the Internet location where it will be posted. 15 CFR §740.13(e)(3).

© The Regents of the University of California

§21.48 d. Related Technology

In addition to the software itself, it may also be necessary to export "technology" associated with it, particularly when jointly developing software with foreign entities or when engaging foreign distributors to market and sell the software. The Export Administration Regulations (EAR) (15 CFR pts 730-774) define "technology" as "[s]pecific information necessary for the 'development,' 'production,' or 'use' of a product. The information takes the form of technical data or technical assistance." 15 CFR §772.1. The regulations state that technical assistance may take forms such as instruction, skills training, working knowledge, and consulting services, and that it may involve the transfer of technical data. The regulations provide that "technical data" may (15 CFR §772.1):

> take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories.

The export of technology often provides a foreign national with the greatest opportunity to understand or reproduce a product.

Exports of technology are generally more regulated than exports of corresponding equipment or software. For example, License Exception ENC does not authorize exports of encryption technology to the "permitted" countries; a license is still required. However, certain license exceptions may be available for technology related to software products. License Exception TSU (Technology and Software Unrestricted) authorizes the export of "operation technology," which is defined as "the minimum technology necessary for the installation, operation, maintenance (checking), and repair" of the underlying products. 15 CFR §740.13(a). This exception also authorizes the export of "sales technology," which is defined as "data supporting a prospective or actual quotation, bid, or offer to sell, lease, or otherwise supply any item." 15 CFR §740.13(b). License Exception TSR (Technology and Software Under Restriction) authorizes the export of technology sufficient for a product's development or production but only to specified countries. See 15 CFR §740.6(a).

NOTE: Encryption technology is subject to special rules, and may not qualify for the license exceptions discussed above. See 15 CFR §§740.13(d)(2), 740.17(b), 742.15(b)(3).

© The Regents of the University of California

§21.49 E. Compliance Measures

A United States company is responsible for ensuring that it does not knowingly violate export controls and must caution recipients of its products and technology not to violate export controls. In addition, the company may wish to take steps to protect itself should export control violations occur without its knowledge. Implementing effective compliance measures requires a company to understand and document its transactions.

© The Regents of the University of California

§21.50 1. Knowledge of Export Control Violations

No export to any country may be made if the exporter has "reason to know" that the item will in turn be reexported to an embargoed country, a prohibited country, a foreign national of one of those countries, or anyone on the lists discussed in §21.52. 15 CFR §§736.1(c), 736.2. The Export Administration Regulations (EAR) (15 CFR pts 730-774) define "knowledge" to include an "awareness" that the future occurrence of a circumstance is "more likely than not." See 15 CFR §772.1. The EAR provides a set of six illustrative due diligence measures that should be undertaken for every export transaction to "know your customer" and to check for "red flags." See 15 CFR pt 732, Supp No. 3 ("Know Your Customer" Guidance). The regulations list a series of indicators, termed "red flags," that should create suspicion that an export control violation may occur. See 15 CFR pt 732, Supp No. 3 ("Red Flags"). If there are no red flags, the exporter can rely on the customer's representations and is under no obligation to verify them or inquire further. If there are red flags, however, the exporter has an affirmative duty to inquire, and must obtain documentary evidence concerning the suspicious aspects of the transaction. If questions still remain, the exporter should not complete the transaction and should advise the BIS. See 15 CFR pt 732, Supp No. 3.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/21 International Issues/§21.51 a. Knowledge of Ultimate Destination

§21.51 a. Knowledge of Ultimate Destination

The exporter is responsible for knowing the ultimate destination of its export. This means the exporter must be aware not only of where its software or technology will be exported, but also where it will be reexported, if applicable. The Export Administration Regulations (EAR) (15 CFR pts 730-774) define a "reexport" as an actual shipment or transmission of items subject to the EAR from one foreign country to another foreign country. A reexport also occurs when technology or source code subject to the EAR is released to a foreign national outside the United States. 15 CFR §734.2(b)(4)-(5). Export or reexport also includes transshipments or transmissions through a country. 15 CFR §734.2(b)(6).

© The Regents of the University of California

§21.52 b. Prohibited End Users

Regardless of the ultimate destination, the exporter must know exactly to whom it is exporting, because United States export controls also prohibit or require licenses for exports to certain "listed" individuals and organizations. The exporter should refrain from hiring, working with, or engaging in any transactions with any individuals or organizations on the following lists:

- Specially Designated Nationals and Blocked Persons List, maintained by the U.S. Department of the Treasury Office of Foreign Assets Control (OFAC), consists of individuals and organizations deemed to represent restricted countries or known to be involved in terrorism and narcotics trafficking. 31 CFR ch V, App A. This list is available at http://www.treas.gov/offices/enforcement/ofac/sdn.
- Denied Persons List, maintained by BIS, consists of individuals who have had their export privileges suspended for either violating export controls or posing a risk of violation. This list is available at http://www.bis.doc.gov/dpl/default.shtm.
- Entity List, also maintained by BIS, is primarily composed of military, government, and scientific research organizations determined by BIS to be involved in or pose a risk of developing weapons of mass destruction. Exports to these entities generally may not be made without a license. 15 CFR pt 744, Supp No. 4. This list is available at http://www.access.gpo.gov/bis/ear/pdf/744spir.pdf.
- Unverified List, also maintained by BIS, consists of organizations that in the past were parties to a transaction with respect to which BIS could not conduct a pre-license check (PLC) or a postshipment verification (PSV), which raises a "red flag." This list is available at http://www.bis.doc.gov/Enforcement/UnverifiedList/unverified_parties.html.
- List of Debarred Parties, maintained by the Department of State Directorate of Defense Trade Controls (DDTC), consists of individuals and organizations that have been convicted of violating the Arms Export Control Act. See 22 CFR §§127.7, 120.27. This list is available at http://www.pmddtc.state.gov/compliance/debar_admin.html.

© The Regents of the University of California

§21.53 c. Prohibited End Uses

The exporter must also be aware of what the export will be used for. The Export Administration Regulations (EAR) (15 CFR pts 730-774) prohibit exports without a license of all products intended for certain end uses. 15 CFR §§736.2(b)(5), 744.1. Such end uses include nuclear, rocket-related, and unmanned air vehicle end uses, and the design, development, production, stockpiling, or use of chemical or biological weapons. See 15 CFR §§744.2(a), 744.3(a), 744.4(a). An exporter should inquire about a potentially prohibited end use if the export is for a military or scientific research application, and should obtain a statement from the customer warranting that the items will not be used for any prohibited purposes.

© The Regents of the University of California

2. Export Transaction Documentation

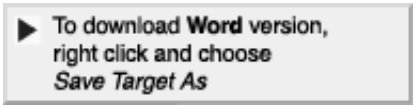
§21.54 a. Automated Export System Record

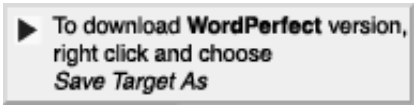
Exporters are required to file an Automated Export System (AES) record (formerly known as a Shipper's Export Declaration (SED) and sometimes referred to as the Electronic Export Information (EEI)) prior to export. 15 CFR §30.2(b). This information is used by the U.S. Census Bureau to calculate export trade statistics, and also by BIS to check whether transactions are in compliance with export controls. 15 CFR §§30.15, 758.1(f). Information regarding AES can be found at http://www.aesdirect.gov. Certain export transactions are exempt from the filing requirement, including:

- Electronic transmissions and intangible transfers (such as e-mail or web download) (15 CFR §30.2(d)(3)); and
- Exports of software and technology that do not require an export license, unless they are mass market (15 CFR §§30.37(f), 758.1(b)(3)).

© The Regents of the University of California

§21.55 b. Destination Control Statement





The shipping documentation accompanying all exports subject to the EAR (except those classified as EAR99) must also include the following Destination Control Statement (DCS) (15 CFR §758.6):

These commodities, technology or software were exported from the United States in accordance with the Export Administration Regulations. Diversion contrary to U.S. law is prohibited.

The DCS must appear on the commercial invoice, and may appear on the export's bill of lading, air waybill, or other export control document that accompanies the shipment. 15 CFR §758.6. For nonphysical exports, such as those made via e-mail or web download, the exporter may display this language on the computer screen for consent before permitting the end user to receive the export.

© The Regents of the University of California

§21.56 c. Contractual Certifications

United States companies may enter into licensing and distribution agreements for their software with third party vendors and customers. Even if the other party to the contract is located within the United States, such licensing and distribution agreements should include provisions stating that the company provided the software within the United States, and that the vendor or customer agrees to not export or reexport the software in violation of U.S. export control laws.

United States companies may also enter into outsourcing agreements with offshore facilities or an onshore facility employing foreign nationals, for the joint development of software or for the sharing of technology. In such a case, the U.S. company should notify the other party of U.S. export controls and obtain certifications that the other party will comply with export controls. Such certifications may include statements that the other party will not reexport any encryption software to a prohibited country (see §21.20) and that it will not release any technology for that software to a foreign national of a prohibited country, including its own employees.

© The Regents of the University of California

§21.57 d. Website Screening System

If a company is planning to sell software products over the Internet, it should establish a procedure on its website to screen prospective purchasers for (1) ultimate destination, (2) end user, and (3) end use. The procedure can require that the purchaser make appropriate certifications before proceeding to the ordering screen, and there should be a mechanism to screen the names, addresses, and affiliations that are entered in the ordering screen.

© The Regents of the University of California

§21.58 e. Access Control System

For exports of encryption software or technology over the Internet that are subject to License Exception ENC, the exporter should also have in place an access control system that checks the address of every non-U.S. party requesting or receiving the software to verify that it does not have a domain name or Internet address of a foreign government, such as ".GOV" or ".MIL." See 15 CFR §734.2(b)(9)(iii)(A). In addition, the posted Destination Control Statement (DCS) (see §21.55) should state that the transfer includes encryption software that may not be exported without authorization. The exporter should also require the recipient to certify that the software is not intended for use by a government end user and that the recipient understands that the encryption software or technology may not be reexported without a license or authorization. 15 CFR §734.2(b)(9)(iii)(C).

© The Regents of the University of California

3. Reporting and Recordkeeping

§21.59 a. Encryption Exports Reports

One of the requirements of License Exception ENC (see 15 CFR §740.17(b), discussed in §21.35) is that the exporter must file semi-annual reports with BIS concerning its exports of these encryption items. See 15 CFR §740.17(e)(1). Certain items and transactions are not subject to the reporting requirements, including encryption items exported to U.S. subsidiaries (see §21.39), products exported to individual consumers that are among those eligible to be exported to government end users, encryption items exported via free or anonymous download, and certain general purpose operating systems or desktop applications (*e.g.,* e-mail, browsers, games, word processing, database, financial applications, or utilities). See 15 CFR §740.17(e)(1)(iii).

© The Regents of the University of California

§21.60 b. Records Maintenance

An exporter of software or technology is required to retain for 5 years detailed records of its transactions, including all export control licenses, applications, documents submitted in support of license applications, memorandums, notes, correspondence, contracts, invitations to bid, books of account, and financial records. The complete list of records required to be retained can be found in 15 CFR §762.2(a).

© The Regents of the University of California

§21.61 4. Export Control Compliance Program

If a company anticipates that the volume or type of its exports will likely increase over time, it should consider implementing an export control compliance program. An export control compliance program should serve to document the company's policies and procedures for export compliance, including identification of controlled items, recordkeeping, screening of future activities, and hiring of foreign nationals who may require an export license.

© The Regents of the University of California

22

Acquisitions and Sales of Internet-Based Businesses

I. INTRODUCTION §22.1

II. PRELIMINARY ISSUES §22.2

III. INTELLECTUAL PROPERTY DUE DILIGENCE
- A. Introduction §22.3
- B. Due Diligence Procedures
  - 1. Confidentiality Agreement §22.4
  - 2. Due Diligence Checklist §22.5
  - 3. Seller's Internal Response Team §22.6
  - 4. Responding to Request §22.7
  - 5. Advance Preparation by Seller §22.8
  - 6. Buyer's Due Diligence Report §22.9
  - 7. Analyzing Information §22.10
  - 8. Disposition of Information §22.11
- C. Sample Due Diligence Checklist
  - 1. Introduction §22.12
  - 2. Checklist: Due Diligence Information Request §22.13
- D. "Open Source" Software
  - 1. Introduction §22.13A
  - 2. Checklist: Acquiring Open Source Software §22.13B
- E. Sample Due Diligence Report
  - 1. Introduction §22.14
  - 2. Checklist: Due Diligence Report re Intellectual Property Matters §22.15

IV. REPRESENTATIONS AND WARRANTIES RE INTELLECTUAL PROPERTY RIGHTS
- A. Introduction §22.16
- B. Form: Representations and Warranties re Intellectual Property §22.17

V. CHANGING OWNERSHIP OF DOMAIN NAMES
- A. Introduction §22.18
- B. Form: Internet Domain Name Assignment Agreement §22.19

© The Regents of the University of California

§22.1 I. INTRODUCTION

This chapter addresses some of the issues involved in acquisition and sale of a website or an Internet-based business, including the buyer's due diligence review of the assets to be transferred (see §§22.3-22.15), typical representations and warranties concerning the seller's intellectual property rights (see §§22.16-22.17), and changing ownership of an Internet domain name (see §§22.18-22.19).

The assets of an Internet-based business fall into several categories, including contract rights, servers and other physical equipment, software, and intellectual property rights, which may include customer lists, stored data, domain names, patents, trademarks, copyrights, and trade secrets. Forms of assignment of intellectual property rights other than domain names can be found in §§1.9-1.11 (copyrights), §§2.15-2.17 (patents), and §§3.56-3.57 (trademarks).

The issues that arise when drafting assignment agreements for various types of intellectual property are similar. The drafter must specifically describe the subject matter of the assignment, and set forth the consideration for assignment, the person responsible for making any necessary filings, and appropriate representations, warranties, and indemnities. The assignment forms in this book range in size and complexity to give the reader a sense of how the documents can be scaled to best fit the circumstances of the transaction at hand.

For a more comprehensive discussion of acquisitions and sales of California businesses, see Sales and Mergers of California Businesses (Cal CEB 2002).

© The Regents of the University of California

§22.2 II. PRELIMINARY ISSUES

Following are some preliminary issues that an Internet-based business and its counsel should consider before entering into negotiations with a prospective buyer for the purchase and sale of the business.

- **Consent of secured creditors.** The seller's counsel should review the covenants and assignment clauses in the seller's loan agreements, equipment leases, and any related personal guaranties to determine what restrictions on sale or transfer exist. Even if the seller is retaining some assets, a transfer of its website may not be possible without obtaining a release of a creditor's security interest. The act of transfer without such consent would likely breach the loan agreement.
- **Consent to assignment of contracts.** The seller's counsel should review all licenses and contracts related to the website and the online business to determine whether they are assignable. These licenses and contracts may include software licenses, support and maintenance agreements, and contracts for web hosting or related services. Typically, these contracts are not assignable without consent of the other party, and the time and potential expense of obtaining consents must be considered in planning the sale of the business.

PRACTICE TIP: Counsel should carefully review all contracts and licenses to determine the impact of transfer, assignment, or change of control on their continued validity. In *Cincom Sys., Inc. v Novelis Corp.* (6th Cir 2009) 581 F3d 431, the court held that the merger of two corporate subsidiaries as part of a corporate restructuring resulted in a transfer of a software license to the new corporate entity, thereby violating the agreement's provision that the license could not be transferred without prior written approval.

- **Privacy issues concerning stored data.** If the website maintains any personally identifiable information on customers or website users, there may be legal or contractual restrictions on transfer of this information to third parties. The website's own privacy policy or applicable law may not permit disclosure of personal information. See chap 9 for a discussion of privacy law and privacy policies.
- **Shutting down the website.** If the seller is no longer operating its website, the website should be closed by taking it offline or posting a notice to the effect that "This site is closed." Leaving the website unmonitored could expose the website owner to risks if there is a potential for ongoing interaction by users, *e.g.,* posting content. Further, there are risks of liability for false advertising if the website continues to advertise a product that is no longer available or if the advertisement is out-of-date and does not reflect current changes in the product or service advertised.

© The Regents of the University of California

III. INTELLECTUAL PROPERTY DUE DILIGENCE

§22.3 A. Introduction

A key element of the value of an Internet-based business is intellectual property. Before closing an acquisition of an Internet business, the buyer and its counsel typically develop and execute a plan to investigate and confirm the nature and ownership of the intellectual property associated with the website. Due diligence investigations are a routine aspect of most business acquisitions. See generally Sales and Mergers of California Businesses §§1.39-1.59 (Cal CEB 2002). They are also an important step in a variety of other business transactions, such as equity investments, joint ventures, loans, technology vendor agreements, intellectual property licenses, and co-development agreements. A company doing business on the Internet may receive due diligence inquiries throughout its existence from a number of sources, including potential investors, lenders, business partners, and purchasers. The company should therefore be prepared in advance to respond such inquiries. Sections 22.4-22.15 provide an overview of the due diligence process as it relates to intellectual property rights.

© The Regents of the University of California

B. Due Diligence Procedures

§22.4 1. Confidentiality Agreement

Due diligence requests often encompass trade secrets or other proprietary and confidential information of the selling company. The company should therefore consider, and negotiate with the buyer, in advance of making any disclosures, the timing and manner of disclosure of such information. If the prospective buyer is a competitor or potential litigant, releasing the information could be detrimental to the company if the buyer does not consummate the purchase transaction. No information should be disclosed unless the prospective buyer first executes a confidentiality agreement to preserve the trade secret status of information disclosed. See chap 2 for a discussion of trade secret law and a sample form of confidentiality agreement. If some disclosures have been made before execution of the agreement, the agreement should be drafted to cover all disclosures from the date first made. The agreement should also cover disposition of the information if the transaction does not close. See §22.11.

© The Regents of the University of California

§22.5 2. Due Diligence Checklist

The exchange of information in a due diligence investigation is typically formalized with an itemized due diligence checklist. The checklist is submitted by the buyer to the seller in writing and may be negotiated by the parties to narrow the scope of the request according to the requirements of the transaction. The scope of the checklist and the items to be investigated may vary depending on the type of transaction, the nature of the intellectual property involved, and the dollar value or exposure to the parties in the transaction. For the sale of a business that depends on key software or patents, extensive investigation may be required to evaluate potential risks to the buyer and to set a reasonable purchase price.

From the selling company's perspective, it is preferable to agree on a formal checklist to govern the due diligence process rather than to receive a series of potentially redundant or conflicting requests for information from different representatives of the buyer. A sample checklist is reproduced in §§22.12-22.13.

© The Regents of the University of California

§22.6 3. Seller's Internal Response Team

On receipt of the checklist, the selling company should assemble a team of individuals in key subject areas (such as legal and technical) to prepare a response. The seller should also designate a due diligence team leader, ideally with some experience conducting or responding to due diligence requests, to serve as the buyer's principal contact. This will assist in efficient information flow and help the seller maintain control over the disclosures made.

© The Regents of the University of California

§22.7 4. Responding to Request

Typically, the selling company assembles the documents and materials containing the information requested and provides copies to the buyer. If confidential information is involved, the documents and materials should be marked as such conspicuously. It is also important to keep copies of all documents furnished to the buyer for purposes of having a record of what has been disclosed if any future questions or disputes arise. If large quantities of documents and materials are involved or if there are a number of potential buyers who wish to inspect the documents at the same time, it is customary for the selling company to establish a "data room" at the company where the documents can be laid out for the convenience of prospective buyers to review and copy. If the documents are confidential, the selling company may wish to restrict copying but permit on-site inspection.

© The Regents of the University of California

§22.8 5. Advance Preparation by Seller

The process of responding to a due diligence request can be laborious for a selling company. It may involve investigation of events that occurred many years in the past or involve employees who are no longer with the company. Moreover, a seller's failure to respond adequately or to respond with an answer that reveals an unexpected potential liability may jeopardize the transaction. Counsel should advise a company to establish a regular practice of compiling and reviewing documents and materials in advance that are likely to be the subject of a due diligence request. The company will thus be in a better position to address and resolve any problems or issues that might arise.

© The Regents of the University of California

§22.9 6. Buyer's Due Diligence Report

A prospective buyer should also assemble a team of experts to review the seller's responses to the due diligence request and report on their findings. The report should summarize the information received, key negative or positive implications, and any open questions. A sample format for a due diligence report is set forth in §§22.14-22.15. The report should reflect the specific purpose of the due diligence investigation. For example, lenders will focus on title, encumbrances, and valuation if the intellectual property is to serve as collateral for a loan. If a prospective buyer intends to integrate the seller's software with other code in another product, then the structure and adaptability of the seller's software becomes more important than its value standing alone.

© The Regents of the University of California

§22.10 7. Analyzing Information

It is important to tie the information obtained from the due diligence investigation back to the original objective of the inquiry. The results of a due diligence investigation may validate the seller's price for the assets or indicate that the price is too high in light of potential risks disclosed in the investigation. Key assumptions that determine the purchase price or support the willingness of the buyer to consummate the transaction should be reflected in the purchase and sale agreement. This is typically achieved by requiring the seller to make representations and warranties that confirm the buyer's factual and legal assumptions underlying the transaction. In addition, if there are due diligence concerns in areas that were not fully investigated prior to closing, representations and warranties on those topics may give the buyer some contractual protection. For samples of typical representations and warranties covering intellectual property, see §§22.16-22.17.

© The Regents of the University of California

§22.11 8. Disposition of Information

When due diligence is complete, the buyer should dispose of documents and materials received from the selling company in accordance with the terms of the confidentiality agreement. Both sides may wish to retain copies of the due diligence materials for reference purposes in the event of a later dispute. If the transaction does not close, however, the seller should not permit a competitor or potential competitor to retain confidential information about the seller. The confidentiality agreement should address the possibility that the transaction might not close and should determine how confidential information regarding the seller will be handled by the recipient in those circumstances.

© The Regents of the University of California

C. Sample Due Diligence Checklist

§22.12 1. Introduction

In §22.13 is a sample due diligence checklist relating to intellectual property assets. In larger transactions such as a sale of an entire business, a venture capital investment, or a joint venture, the checklist in §22.13 would be one part of a larger checklist covering the target company's entire operations. Counsel should note that the list below does not cover technological or security issues that may be relevant to a website's operations.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/22 Acquisitions and Sales of Internet-Based Businesses/ §22.13 2. Checklist: Due Diligence Information Request

§22.13 2. Checklist: Due Diligence Information Request

▶ To download **Word** version, right click and choose *Save Target As*

▶ To download **WordPerfect** version, right click and choose *Save Target As*

DUE DILIGENCE INFORMATION REQUEST

1. Trademarks

- List of service marks, service names, trademarks and trade names, trade dress, business and product names, logos, and slogans.
- Are any of the above marks registered? If so provide registration number, date, and jurisdiction of registration. Provide copies of all trademark registration certificates.
- Are any of the above marks subject to pending applications for registration? If so, provide application number, date, jurisdiction, and current status of pending application. Provide copies of all trademark applications for registration and related correspondence.
- Have any trademarks or applications for trademark registration been denied, cancelled, or opposed? Provide applicable mark, date of action, opposing party, description, and status of matter.

2. Patents

- List of registered patents in all jurisdictions, registration number, date, and jurisdiction of registration. Provide copies of all registered patents.
- List of all pending applications for patent registration in all jurisdictions, application number, date, and jurisdiction of registration. Provide copies of all applications for registration and related correspondence.
- Have any patents or applications for patent registration been denied, cancelled, or opposed? Provide applicable patent or application, date of action, opposing party, description, and status of matter.

3. Copyrights

- List of registered copyrights in all jurisdictions, registration number, date, and jurisdiction of registration. Provide a copy of all copyright registration certificates.
- List of all pending copyright filings in all jurisdictions.

4. Software

- List of computer programs (including all source code) and related documentation in which the company has an ownership interest. If software is jointly owned, list names and contact information for co-owners and provide copies of any co ownership agreements.
- List of computer programs (including all source code) and related documentation which the company has licensed from third parties. Provide copies of all software licenses.
- List of all software escrow agreements to which the company is a party, along with the other parties to the escrow (including the escrow agent), a description of the software in escrow, and copies of such agreements.

5. Internet Website(s)

- List of all domain name registrations held by the company.
- Identify the persons or entities that developed the website initially and that have performed any modifications and upgrades. Provide copies of all development and related agreements.
- Is the Internet website hosted by a third party? Provide copies of all hosting and related agreements.
- Provide copies of all terms of use and privacy policies, including any amendments, for the website that have been posted or otherwise used at any time during the past 5 years.

- Have any of the domain names been contested for trademark infringement? If yes, provide a detailed summary and status.
- Have any notices been received regarding the potential infringement of third party or subscriber-posted content on the site? If so provide a detailed summary and status.
- Provide copies of all internal policies relating to the management of the site including, for example, policies regarding:
- the handling of personally identifiable data;
- the management and maintenance of e-mail lists and the dissemination of promotional e-mail correspondence; and
- the handling of third party notices regarding potentially infringing copyrighted works or trademarks posted on the site or uploaded by end users.
- Identify categories of personally identifiable third party information maintained and locations where the information is maintained. Describe how the information is used and how access to the information is restricted.
- Has personal information from non-U.S. individuals been collected or acquired? If so, identify the countries in which those individuals reside.
- Has any personal information collected been sold, transferred, or made available to third parties? If so, describe the relationship, the third party use of the data, and provide any agreements governing the third party's permitted use of that data.
- Has mass e-mail been used to communicate with customers or potential customers? If "yes," provide sample texts of such communications, including "opt out" procedures.
- Identify any special-purpose privacy laws applicable to the business such as the Gramm-Leach-Bliley Act (covering information held by financial institutions) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (covering health-related information held by certain health care entities). Provide information regarding applicable compliance policies and procedures.

6. Contracts and Licenses

- Provide a list and copies of all assignments and licenses of intellectual property rights to third parties, indicating when and where such rights became effective.
- Provide a list and copies of all assignments and licenses of intellectual property from third parties, indicating when and where such rights became effective.
- Provide copies of all agreements with employees and independent contractors covering development of intellectual property, together with a list of employees and independent contractors subject to these agreements if not shown on the copy.
- Provide copies of all agreements with third parties for the design, development, programming, enhancement, or maintenance of any of the company's intellectual property.
- Security interests
- Is the company subject to any security interest, lien, or other encumbrance on any of its intellectual property or "general intangibles"? If so, provide the name of the lienholder, the date of the lien, description of collateral, and term of lien.
- Is any computer software or other work of the company subject to any security interest, lien, or other encumbrance? If so, provide the name of the lienholder, the date of the lien, description of collateral, and term of lien.

7. Litigation

- Provide copies of any communications to or from third parties relating to the validity or infringement of company's patents, technology, trade secrets, trademarks (service marks), trade dress, and copyrights.
- List all litigation related to intellectual property of the company in the past 5 years, including names of parties, description of the claims made, and status of the claims.
- List all litigation brought by the company in the past 5 years related to intellectual property issues, including names of parties, description of the claims made, and status of the claims.

8. Miscellaneous

- Provide names of and contact information for all current outside trademark, copyright, and patent counsel.
- Provide copies of all material correspondence during the past 5 years with the U.S. Patent and Trademark Office, the U.S. Copyright Office, or any other comparable regulatory agency.
- Describe any intellectual property insurance held. Have there been any claims against such policies in the past 5 years?

9. For _ _[*identify key works, such as the target's main software product*]**_ _, provide more detailed information as follows:**

- How did the work come to be in the possession of the company?
- Identify all persons who authored or invented the work (or who might claim to have authored or invented the work) and describe the role that each played in the authorship or invention.
- Were all of the employees who developed the work subject to written employment agreements? What is the current employment status of each such employee? Provide a copy of all employment agreements. Identify any employees who were not subject to written employment agreements.
- Was the independent contractor or consultant subject to a written agreement before developing the work? Provide a copy of such agreements.
- Did any customer of the company pay for development of the work or supply anything that was incorporated in the work? Did the customer supply any prior work of authorship or prior art that was incorporated in the work or invention developed by the company? Provide a copy of any agreement with such customer granting the right to do so.
- Was anything developed by a third party used to develop the work? Did the company acquire anything that was incorporated in the work by license, assignment, or other transfer? Provide a copy of the relevant agreements.
- Is the company aware of any third party who might claim that use or dissemination of the work might infringe its copyrights, patents, trade secrets, or other intellectual property rights?
- Was any work or portion of it produced under contract for or licensed to any government agency?

© The Regents of the University of California

D. "Open Source" Software

§22.13A 1. Introduction

Recent years have witnessed the growth of "open source" software, such as Linux, the source code for which is freely available to all under a variety of licensing models designed to preserve the code in the public domain. See, *e.g.,* the GNU website at http://www.gnu.org/licenses/licenses.html for sample open source license agreements. Open source provides many benefits, among them the ability of any user, anywhere, to recommend bug fixes and provide a "virtual" support team. Further, using open source may lower a startup business's product development costs.

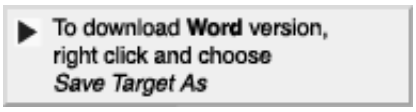
A number of open source licenses permit use of the open source software only if a software distributor makes publicly available the source code of all derivative or collective works that include the open source code. See GNU General Public License at http://www.gnu.org/licenses/gpl.html. See generally http://www.opensource.org. Open source license programs are often designed to ensure that code modifications are available to the community in source code form without charge. An established commercial software company will not want a target seller's use of open source software to require the release of source code for its own proprietary products. Acquiring companies, therefore, will want to know that any use of open source software has been carefully tracked and controlled so that an obligation to release source code arises only in situations where intended.

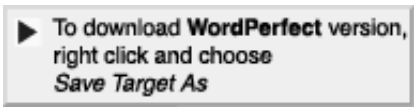
Because open source software can be downloaded without charge, it can evade the internal business procurement controls typically in place for commercial purchases. The open source code often comes in through the "back door" and, if untracked, can taint a company's products.

PRACTICE TIP: When performing due diligence in connection with the potential acquisition of a software company, the seller's source code and the trade secrets associated with it are typically among the most valuable assets. Inappropriate use of open source software programs in development of the seller's products, however, may raise serious concerns about the proprietary nature of the seller's code, and result in a significant decrease in the buyer's estimate of the value of the target company's technology.

© The Regents of the University of California

§22.13B 2. Checklist: Acquiring Open Source Software





- 1. Does the seller have an open source policy regarding the use and tracking of open source and compliance with license terms? Are "code reviews" conducted to determine whether any open source elements have been integrated into the products? How is the policy communicated and enforced?
- 2. Identify any inbound open source licenses and determine if the code was actually used or embodied in the seller's products.

Comment: This assessment may require a detailed technical understanding of the seller's products and may require expert assistance. The buyer should review the seller's code base and search its code for indications of open source software usage. Some programs search all text strings for specific words associated with free and open source software, such as GNU, GPL, and Linux. Other programs attempt to identify object code that is identical to code found in these programs.

- 3. Do the affected products represent a substantial source of revenue to the seller? Are the affected products part of an integrated software solution or suite of products sold to third parties or are they used only internally?
- 4. Review the terms of any applicable open source licenses to determine the specific requirements. There are many types of open source licenses, many of which have standard terms that have varied over time.
- 5. Assess whether the seller is in compliance with the terms of any applicable open source licenses.
- 6. Determine the effect of the existence of open source code on the available warranties for the seller's software.

PRACTICE TIP: Contributors to an open source project are usually not asked to make warranties about the originality of their code, and often contribute to the software project while employed by corporations that can make claims to the code as a work for hire. Sellers are therefore often reluctant to make representations about open source software. Buyers should, at a minimum, seek a representation that the facts relevant to the seller's compliance with the terms of open source licenses are true.

© The Regents of the University of California

D. Sample Due Diligence Report

§22.14 1. Introduction

After due diligence materials have been received and analyzed by representatives of the buyer, the results of the analysis are summarized and provided to the buyer's management. Set forth in §22.15 is a format for a report concerning intellectual property due diligence matters.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/22 Acquisitions and Sales of Internet-Based Businesses/ §22.15 2. Form: Due Diligence Report re Intellectual Property Matters

§22.15 2. Form: Due Diligence Report re Intellectual Property Matters

▶ To download **Word** version, right click and choose *Save Target As*

▶ To download **WordPerfect** version, right click and choose *Save Target As*

REPORT OF RESULTS OF PRELIMINARY DUE DILIGENCE INQUIRY

INTELLECTUAL PROPERTY (PATENTS, TRADEMARKS, COPYRIGHTS, AND TRADE SECRETS)

Name of Target: _____

Date:_____

Individuals Providing Report: _____

_____

1. TRADEMARKS

Registrations Reviewed

[*List the target's registered trademarks and provide key data such as name, class of registration, due date for next payment, and any disclaimers.*]

[*List applications for registration and status.*]

Unregistered Marks

[*List any unregistered marks used and results of preliminary trademark search on such marks, and any other issues.*]

Domain Names

[*List domain names and describe any concerns regarding trademark protection for same.*]

Licenses

[*List key trademark license agreements. Summarize the basic terms of any trademark licenses of the company's marks, royalty payment terms, and status of payments. Do the same for any licenses of third party trademarks held by the company. Are these agreements assignable? Should the buyer take an assignment?*]

[*Describe any weaknesses in controls on third party licensee's use of marks and quality of use.*]

Key Issues

[*Identify key issues of strength and weakness, and discuss any impact on purchase price or valuation.*]

2. COPYRIGHTS

Registrations Reviewed

[*List the seller's registered copyrights.*]

[*List applications for registration and status.*]

Unregistered Works

[*List key works that are unregistered, including any amendments, modifications, or upgrades to registered works.*]

Licenses

[*List key copyright license agreements. Summarize the basic terms of any license of the company's copyrighted works, royalty payment terms, and status of payments. Do the same for licenses of third party copyrights held by the company. Are these agreements assignable? Should the buyer take an assignment?*]

Key Issues

[*Identify key issues of strength and weakness, and discuss any impact on purchase price or valuation.*]

3. SOFTWARE

List

[*List key elements of software and indicate which are owned by the company, which are co-owned, and which are licensed from third parties.*]

Protection

[*Describe how the company protects its rights in the software. By copyright? Patent? Trade secret? Assess strength of that protection.*]

Licenses

[*List key agreements. Summarize the basic terms of any licenses of the company's software, royalty payment terms, and the status of payments. Do the same for licenses of third party software (including open source licenses) held by the Company. Are these agreements assignable? Would the buyer want to take an assignment?*]

[*Are there any source code escrow arrangements? Describe.*]

Miscellaneous

[*Describe any software developed for the government.*]

[*Describe any software subject to export control.*]

Key Issues

[*Identify key issues of strength and weakness, and discuss any impact on purchase price or valuation.*]

4. PATENTS

Registrations Reviewed

[*List the target's patent registrations and provide key data such as name, due date for next payment, any disclaimers, limitations, or weaknesses.*]

[*List applications for registration and status.*]

[*Determine whether to obtain patent counsel evaluation of prior art and strength of portfolio.*]

Unpatented inventions

[*List any key inventions or business processes that remain unpatented.*]

Licenses

[*List key agreements. Summarize the basic terms of any licenses of the company's patents, royalty payment terms and status of payments. Do the same for licenses of third party patents held by the company. In each case, how are intellectual property rights allocated? Are these agreements assignable? Would the buyer want to take an assignment?*]

Key Issues

[*Identify key issues of strength and weakness, and discuss any impact on purchase price or valuation.*]

5. POLICIES

Ownership Issues

[*Describe invention disclosure policy for employee-created inventions.*]

[*Describe policy regarding unsolicited idea submission by third parties.*]

[*Discuss strength and weakness of employee and contractor invention assignments.*]

[*Are there any major issues with the chain of title or proving intellectual property ownership that have not yet been discussed?*]

Internet

[*Describe any issues with privacy policy, terms of use, or other web policies.*]

Key Issues

[*Identify key issues of strength and weakness, and discuss any impact on purchase price or valuation.*]

6. LITIGATION

Summary of Status

[*Summarize any material present litigation.*]

[*Summarize any material past litigation.*]

Key Issues

[*Identify key issues of strength and weakness, and discuss any impact on purchase price or valuation.*]

© The Regents of the University of California

IV. REPRESENTATIONS AND WARRANTIES RE INTELLECTUAL PROPERTY RIGHTS

§22.16 A. Introduction

The seller of an Internet business can expect the prospective buyer to request that the purchase agreement include representations and warranties concerning the ownership and status of all intellectual property rights associated with the website. The content of the representations and warranties and the extent to which they are subject to qualifications will vary with the transaction and the relative bargaining power of seller and buyer. In §22.17 is a sample set of intellectual property representations and warranties. For further discussion and samples of all representations and warranties typically included in business acquisition agreements, see Sales and Mergers of California Businesses (Cal CEB 2002).

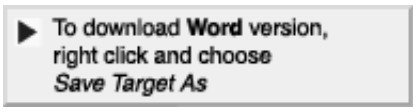
Although representations and warranties provide comfort to the purchaser and may provide a contractual cause of action in the event of a breach, practitioners should be aware that obtaining representations and warranties without confirmatory due diligence may not be sufficient to protect purchasers against a regulatory violation. For example, the New York Attorney General obtained a $1.1 million settlement in a suit against Datran Media, LLC, an e-mail marketer, who purchased consumer lists from third parties for direct e-mail marketing purposes. The Attorney General found that Datran purchased lists from sellers who had specifically represented that they would not share consumers' e-mail addresses, and that Datran used the information it purchased in violation of those representations. According to the Attorney General, Datran either knew of or could have easily have learned of these practices, because the sellers' websites contained public promises not to share information. The terms of the settlement require Datran to "avoid acquisition of any personal consumer information without first independently confirming that such acquisition is permissible under relevant seller privacy policies." See http://www.oag.state.ny.us/media_center/2006/mar/mar13a_06.html.

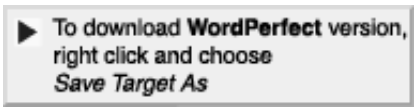
NOTE: Counsel should advise clients purchasing assets that include customer lists and customer information not to rely on the seller's assurances that the lists and information can be freely used. Instead, the buyer should be advised to obtain copies of the relevant policies and agreements (from the seller and any third parties) under which the names and other customer information were obtained. If customers were promised that their e-mail addresses and other personal information would not be shared, then the buyer may not use that information and the seller's representation to the contrary may not provide an effective shield against liability to the customers. Buyers should review the privacy policy and other statements posted on the website of the party that obtained the information and search for language that explains to consumers how collected information would be used. It is important to note the date when the information was obtained and verify that the relevant policies and language were in effect at that time, because data collection and privacy policies may have changed.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/22 Acquisitions and Sales of Internet-Based Businesses/ §22.17 B. Form: Representations and Warranties re Intellectual Property

§22.17 B. Form: Representations and Warranties re Intellectual Property





The Company represents and warrants as follows:

(a) Except as set forth on Exhibit A, the Company owns, or otherwise has the right to use, all copyrights, patents, patent applications, inventions, know-how, processes, technology, trademarks, service marks, trade names, trade name rights, trade secrets, domain names, Uniform Resource Locators ("URLs"), and other intangible intellectual property rights (collectively, the "IP Rights") used in its business as now conducted.

Comment: From the selling company's perspective, it is preferable to make only representations and warranties that are relatively easy to prove. A representation that the company owns all intellectual property that it *uses* in connection with its business may be hard for the company to investigate and confirm internally. While this representation provides comfort to the buyer, the company should verify that it has an internal inventory of the intellectual property it uses.

From the buyer's perspective, the qualifier concerning the business of the company "as now conducted" might be too limiting. If the company operated its business using infringing intellectual property in the recent past, the buyer might be exposed to the risk of infringement claims. The company, however, may not be willing to remove the qualifying phrase, either because it does not have an inventory of intellectual property used in the past or because of management turnover.

(b) Exhibit A contains a complete list of all patents, patent applications, copyright registrations, copyright applications, significant works of authorship in which copyright is claimed, trademarks, service marks, trademark and service mark registrations, applications for trademark and service mark registrations, domain names, and root URLs that are used in the Company's business as now conducted.

Comment: Sometimes, a buyer asks the selling company to list all of its intellectual property, including all of its trade secrets and all unregistered copyrights. Such a list may be almost impossible to create, because in theory it would include a broad range of previously unrecorded thoughts, concepts, and business processes. It would therefore be difficult for a company to give such a representation without being in breach at the time it signs the agreement.

(c) Except as shown on Exhibit A, there are no outstanding options, licenses, or agreements of any kind relating to the Company's IP Rights, nor is the Company bound by or a party to any options, licenses, or agreements of any kind with respect to the IP Rights of any third party, other than off-the-shelf end-user licenses.

Comment: The term "off-the-shelf end-user licenses" is intended to refer to nonnegotiated licenses for commercially available software, such as word processing or spreadsheet programs or computer operating systems.

(d) To the Company's knowledge, the Company has not received any communications or claims alleging that the Company has interfered with, infringed upon, misappropriated, or otherwise come in conflict with the IP Rights of any third party.

Comment: While the selling company may assert that it is reasonable to limit this representation to the company's knowledge, the buyer may insist on a different formulation. Another way of qualifying the representation is to state that the company is not "aware" of any infringement or misappropriation claims. If there are any claims, they can be listed on Exhibit A. The buyer, however, may request an unqualified representation that there is no pending litigation and that the company has received no notice of any infringement claims. If the company's website includes areas for posting or uploading of content by end users or subscribers, a representation should be added that no notice of the potential infringing nature of such third party posted or uploaded content has been received, and, if received, all applicable laws have been complied with in connection with the handling of the notice. Consider requiring the seller to list all open and

unresolved notices of potentially infringing third party content posted on the website or uploaded to the seller's network.

(e) The Company has complied in all material respects with all of its obligations of confidentiality in respect of claimed trade secrets or proprietary information of others and has no knowledge of any material violation of any obligations of confidentiality to which the Company is subject.

Comment: This representation is qualified by materiality standards, which may or may not be reasonable depending on the circumstances. For example, if the company is required to safeguard highly confidential information (such as hospital records or insurance information) for its customers, the buyer should insist that this representation not be qualified by materiality.

(f) Each current and past officer, employee, and consultant of or to the Company has, for adequate consideration, executed and delivered to and in favor of the Company the Company's standard form of agreement regarding the protection of confidential and proprietary information and the assignment to the Company of all IP Rights arising from the services performed for the Company by such person.

Comment: The selling company may have used more than one standard form of confidentiality agreement in its history. If so, the buyer may ask the company to attach samples of the forms used or to state that all of the forms used contain certain minimum requirements. The company may also be asked to list on Exhibit A any employees or consultants who have not signed the standard form.

(g) No employee, agent, or consultant of the Company is subject to confidentiality restrictions in favor of any third party, the breach of which could subject the Company to any material liability.

Comment: This is another representation that may be difficult for the selling company to verify. The company may not be aware of all the confidentiality restrictions that its employees or consultants have agreed to in the past. The company should therefore ask that this representation be limited to the company's knowledge.

(h) All of the Company's IP Rights (with the exception of those under pending patent and intent-to-use trademark applications) are valid and in full force and effect.

Comment: The company may not be in a position to know this information completely. For example, a trade secret or unpatented business process it uses may be infringing a third party patent the company is unaware of or an unregistered trademark used by it may be limited by a prior substantially similar third party mark the company is unaware of. This representation could be limited to registered intellectual property rights or perhaps limited to knowledge.

(i) The Company has taken all steps customary and reasonable in the industry to protect and preserve the confidentiality and proprietary nature of the Company's IP Rights.

Comment: This clause may be too vague to work in all circumstances. Consider whether there is a baseline of actions that the company may be willing to represent to. For example, that access to source code for its key valuable software has been restricted and tracked in a certain fashion.

(j) Except as disclosed in Exhibit A, (1) there are no licenses or other similar agreements to which the Company is a party or by which it is bound pursuant to which it has granted exclusive license rights in or with respect to the Company's IP Rights, and (2) there are no licenses or similar agreements pursuant to which the Company has received license rights in or with respect to the IP Rights of any third party licensor, which licenses or similar agreements require the consent of such licensor to the transfer thereof to Buyer.

Comment: Clause (1) of this representation requires listing only exclusive licenses. In many circumstances, the buyer would want all licenses listed. There may be a separate representation and warranty elsewhere in the agreement with respect to all material contracts of the company that requires a listing of these agreements already. If so, all the license agreements would likely be listed there.

(k) The Company has at all times complied with all applicable laws and any internal privacy policies relating to (1) the privacy of information regarding the users of its products, services, and all Internet sites owned, maintained, or operated by the Company and (2) the collection, storage, and transfer of any personally identifiable information by the Company or by third parties having authorized access to the records of the

Company. The execution, delivery, and performance of this Agreement does not violate any applicable laws relating to privacy and does not violate the Company's privacy policies. Accurate and complete copies of all current and prior privacy policies of the Company are included in Exhibit A. Each such privacy policy and all materials distributed or marketed by the Company have at all times made all privacy-related disclosures to users or customers required by applicable laws, and none of such disclosures have been inaccurate, misleading, or in violation of any applicable laws. With respect to all personal and user information described in this subsection (k), the Company has at all times taken all steps reasonably necessary to protect the information against loss and against unauthorized access, use, modification, or disclosure. To the Company's knowledge, there has been no unauthorized access, modification, disclosure, or other misuse of such information.

Comment: This example of a representation and warranty regarding compliance with privacy laws and privacy policies must be tailored to the specific circumstances of the seller and its business. For example, if the seller operates outside of the United States, the language should be broadened to include applicable foreign laws and accords. If the seller is in a regulated industry, such as the financial or health care industry, special privacy laws may apply. See chap 9. Consider describing, or requiring the Company to describe, in Exhibit A the types of protections the Company is expected to have in place to protect private data, including physical security measures, passwords, and technical security measures such as firewalls and encryption.

© The Regents of the University of California

V. CHANGING OWNERSHIP OF DOMAIN NAMES

§22.18 A. Introduction

For a comprehensive discussion of Internet domain names, including registration procedures and domain name infringement, see §§3.1-3.24. To change the ownership of a domain name, the first step is to contact the domain name registrar to determine the current procedures and the required forms and fees. Often the change can be made at no charge or only a nominal charge. With some registrars, the ownership change can be made by logging into the account manager portion of the registrar's website and revising the ownership screen to effect the change in real time. The change is typically irreversible, and once ownership has changed, the former owner relinquishes all rights to the domain name and no longer has access to the domain record.

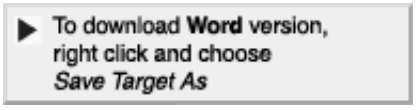
Typically, only the domain name owner or its authorized representative can transfer or sell the domain name. This is important because businesses often do not focus on how the domain name owner is listed with the registrar and whether it is listed correctly. Sometimes, companies permit their web developer, website host, or an employee or consultant to obtain the domain name with the intent of later transferring it to the company. If that transfer does not take place and the company desires to sell the domain name, it will have a difficult time doing so, especially if the listed owner no longer has a relationship with the company and is difficult to locate.

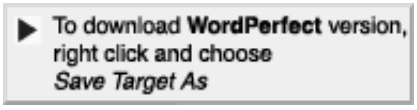
NOTE: Practitioners should be aware that, in the lexicon of Internet registries, a domain name "transfer" or "assignment" means to move a domain name from one registrar to another registrar without changing ownership. It merely signifies a change in service provider. A "change in ownership" is the terminology most often used if the intent of the parties is to divest the owner of all rights in the domain name.

The actual change in ownership is effected by submitting the required forms to the registrar of the domain name. Those forms, however, are merely instructions to the registrar and do not define the terms and conditions of the sale between the parties. Therefore, the parties typically also enter into a separate form of domain name assignment agreement, such as the one set forth in §22.19.

© The Regents of the University of California

§22.19 B. Form: Internet Domain Name Assignment Agreement





INTERNET DOMAIN NAME ASSIGNMENT AGREEMENT

THIS INTERNET DOMAIN NAME ASSIGNMENT AGREEMENT (this "Agreement") is entered into between _ _[*name of Seller*]_ _**, located at** _ _[*address of Seller*]_ _ **("Seller"), and** _ _[*name of Buyer*]_ _**, located at** _ _[*address of Buyer*]_ _ **("Buyer"), as of** _ _[*date*]_ _**, with reference to the following facts:**

A. Seller is the owner of the Internet Domain Name _ _[*domain name*]_ _ **("Domain Name") as listed in the records of** _ _[*name of registrar*]_ _ **registrar of record (the "Registrar"), and is the owner of all common law trademark rights derived from the Domain Name as well as all copyright and other intellectual property or other proprietary rights based on or related to the Domain Name; and**

B. Buyer desires to purchase the Domain Name and all common law trademark and service mark rights derived from the Domain Name, as well as all copyright and other intellectual property or other proprietary rights based on or related to the Domain Name (the "Intellectual Property Rights").

NOW, THEREFORE, in consideration of the promises made in this Agreement and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties agree as follows:

1. DOMAIN NAME ASSIGNMENT.

1.1. ASSIGNMENT OF DOMAIN NAME. Seller hereby agrees to transfer and assign to Buyer at the Closing all of Seller's right, title, and interest in and to the Domain Name and the registration thereof, any domain names that are foreign language versions of the Domain name or misspellings of the Domain Name, together with the goodwill of the business connected with and symbolized by such Domain Name, and the Intellectual Property Rights, which include the trademark and the service mark _ _[*description of trademark or service mark*]_ _**. The transfer and the assignment shall take effect at the Closing upon Buyer's making payment in full as provided for herein.**

1.2. COOPERATION IN TRANSFERRING DOMAIN NAME. Seller agrees to cooperate with Buyer and to follow Buyer's reasonable instructions in order to effectuate the transfer of the Domain Name registration in a timely manner. Specifically, at the Closing Seller agrees to prepare and transmit the necessary Registrant Name Change Agreement (NCA) and to correspond with the Registrar to authorize transfer of the Domain Name, effective as of the Closing Date as hereinafter defined.

1.3. WARRANTY. Seller warrants and represents that it has unencumbered rights in the Domain Name, that Seller properly registered the Domain Name with InterNic without committing fraud or misrepresentation, that Seller has the authority to transfer the Domain Name, and, that to the best of Seller's knowledge, the Domain Name does not infringe the rights of any third party.

2. PURCHASE PRICE. Buyer agrees to pay Seller at Closing an amount equal to _ _[*dollar amount*]_ _ **via** _ _[*specify payment method such as cashiers' check or wire transfer in immediately available funds to an account designated by Seller*]_ _ **as full consideration for the transactions contemplated hereby.**

3. CLOSING.

3.1. CONDITIONS TO BUYER'S OBLIGATION TO CLOSE. The Buyer's obligation to consummate the transactions contemplated by this Agreement at the Closing are subject to completion of the following:

(a) TRANSFER OF DOMAIN NAME. Seller shall have delivered to Buyer all documents necessary to cause the

Domain Name and the registration thereof, together with the goodwill of the business connected with by such Domain Name, the trademark and the service mark "_ _[*specify trademark or service mark*]_ _" and any intellectual property rights relating thereto to be transferred to Buyer. Such documents shall contain no omissions and shall be fully executed by authorized officers of Seller, such that the only remaining step to be taken by Buyer to accomplish the transfer of the Domain Name and the registration therefor from Seller to Buyer is the Buyer's filing of such documents with the appropriate third parties.

(b) REPRESENTATIONS, WARRANTIES, AND COVENANTS. The obligations of Seller required to be performed at or prior to the Closing shall have been performed and complied with in all material respects, and the representations and warranties of Seller set forth in this Agreement shall be true and correct in all respects as of the date of Closing as though made on and as of the date of Closing.

3.2. CONDITIONS TO SELLER'S OBLIGATION TO CLOSE. The Seller's obligation to consummate the transactions contemplated by this Agreement at the Closing are subject to completion of the following:

(a) PAYMENT OF PURCHASE PRICE. The Seller shall have received full payment from Buyer of the purchase price set forth in Section 2.

(b) REPRESENTATIONS, WARRANTIES AND COVENANTS. The obligations of Buyer required to be performed at or prior to the Closing shall have been performed and complied with in all material respects, and the representations and warranties of Buyer set forth in this Agreement shall be true and correct in all respects as of the date of Closing as though made on and as of the date of Closing.

3.3. PLACE AND DATE OF CLOSING. After satisfaction of conditions above, the Closing shall take place at the California offices of the Seller on or before _ _[*date*]_ _. If the Closing does not take place on or before such date, then this Agreement shall terminate and the rights and obligations of the parties to this Agreement shall be of no further force and effect provided that no party hereunder shall be relieved of any breach of this Agreement occurring prior to such termination date. At Closing, each party shall deliver to the other such payments, documents, certificates, consents, approvals, and waivers that shall be reasonably necessary to consummate the obligations of the parties hereunder.

4. EXPENSES. Each party to this Agreement shall bear all of its expenses incurred in the performance hereof, regardless of whether the transactions contemplated herein are consummated.

5. COOPERATION. The parties agree that after Closing they shall provide each other with reasonable cooperation with respect to the transactions that are the subject matter of this Agreement.

6. CONFIDENTIALITY AND PRESS RELEASE.

6.1. Neither party shall, without the consent of the other, disclose the provisions of this Agreement to any third parties (other than as may be required by law, in connection with legal or administrative proceedings, or to attorneys, accountants, and consultants they may have retained to represent them in connection herewith), and this provision shall survive the Closing. There will be no press release or public announcement of this Agreement except as agreed in writing between the parties.

7. MISCELLANEOUS.

7.1. CHOICE OF LAW AND VENUE. This Agreement shall be construed in accordance with the laws of the State of California without regard to its conflicts of laws rules.

7.2. INDEMNITY. Each party hereto agrees to indemnify, defend and hold the other party, its officers, directors, agents, employees and assigns, harmless from and against any claims, damages, losses, costs and expenses resulting from third party claims or arising from breach by any party hereto of its representations, warranties or covenants, contained in this Agreement.

7.3. SECTION HEADINGS. The section headings contained herein are for convenience of reference and are not intended to define or limit the scope of any provision of this Agreement.

7.4. COUNTERPARTS. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, and will become effective and binding on the parties as of the execution date.

7.5. NOTICES. All notices required or permitted to be given hereunder by either party to the other shall be given in writing: (a) by personal delivery; (b) by electronic facsimile with confirmation sent by United States first class registered or certified mail, postage prepaid, return receipt requested; (c) by bonded courier or by a nationally recognized overnight delivery company; or (d) by United States first class registered or certified mail, postage prepaid, return receipt requested, in each case, addressed to the parties as follows (or to such other addresses as the parties may request in writing by notice given pursuant to this section):

Buyer:
_ _[*Name*]_ _
_ _[*Address*]_ _
_ _[*City, state, zip*]_ _

Seller:
_ _[*Name*]_ _
_ _[*Address*]_ _
_ _[*City, state, zip*]_ _

Notices delivered by personal delivery shall be deemed received on the receipt thereof and notices delivered by U.S. mail shall be deemed received 72 hours following deposit in the U.S. mail.

7.6. ENTIRE AGREEMENT. This Agreement contains the entire agreement between the parties with respect to the subject matter of this Agreement, and it supersedes all other prior and contemporary agreements, understandings, and commitments between the parties with respect to the subject matter of this Agreement.

7.7. SUCCESSORS AND ASSIGNS. This Agreement is binding on and shall inure to the benefit of the respective successors and/or assigns of the parties.

IN WITNESS WHEREOF, the parties hereto have executed and delivered this Agreement on the dates written below:

Date: _ _ _ _ _ _

_ _[*NAME OF ASSIGNOR*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

Date: _ _ _ _ _ _

_ _[*NAME OF ASSIGNEE*]_ _,
a _ _[*specify entity, e.g., California corporation*]_ _

By: __[*Signature*]__
Name: _ _[*Typed name*]_ _
Its: _ _[*Title*]_ _

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/Internet Resources for California Businesses

Internet Resources for California Businesses

A. Government Sites—Federal

Americans with Disabilities Act	http://www.ada.gov Information and technical assistance on the ADA by the U.S. Department of Justice.
Board of Governors of the Federal Reserve System	http://www.federalreserve.gov/ Home page with informational links about the "Fed," monetary policy, banking regulation, economic data, and other topics.
Bureau of Industry and Security (BIS), U.S. Department of Commerce	http://www.bis.doc.gov/about/index.htm Federal agency that administers the U.S. export control and treaty compliance system, including the Export Administration Regulations (EAR).
Business.gov	http://www.business.gov/ Home page, operated by the U.S. Small Business Administration, with links to legal and regulatory information, and plain-English guides for starting a business, handling finances, managing employees, and other topics.
CIA, The World Factbook	https://www.cia.gov/library/publications/the-world-factbook/ U.S. government profiles of countries and territories around the world.
Equal Employment Opportunity Commission (EEOC)	http://www.eeoc.gov/ EEOC site with basic introduction to employers' rights and responsibilities under the federal equal employment opportunity laws.
Federal agencies (through Library of Congress site)	http://www.loc.gov/rr/news/fedgov.html A Library of Congress resource page with links to most federal agencies.
Federal Citizen Information Center (FCIC)	http://www.pueblo.gsa.gov/ Part of the U.S. General Services Administration, the FCIC's Small Business Links offer information for persons planning or owning small businesses, including information on procurement, taxes, woman- and minority-owned businesses, human resources, and financial and legal issues.
Federal Deposit Insurance Corporation (FDIC)	http://www.fdic.gov/ Home page with links to statistical data, pertinent regulations, and FAQs.
Federal Register	http://www.gpoaccess.gov/fr/index.html Main page, with search functions, for the Federal Register—the official daily publication for federal agency rules, proposed rules, and notices as well as executive orders. Specific Federal Register pages can be retrieved at http://www.gpoaccess.gov/fr/retrieve.html
Federal Reserve Bank of San Francisco	http://www.frbsf.org/ Home page. The current FRBSF discount rate, used to determine the usury ceiling in California, is posted at http://www.frbsf.org/banking/data/discount/index.html
Federal Trade Commission	http://www.ftc.gov/ftc/business.shtm Home page for businesses, with links to business publications, advertising guidance, fair packaging and labeling, antitrust law guide, and other topics. Information concerning the Hart-Scott-Rodino premerger notification requirements is at http://www.ftc.gov/bc/hsr/introguides/introguides.htm
USA.gov	http://www.usa.gov/Business/Business_Gateway.shtml

	The official web portal of the U.S. government, with links to information on contracting with the U.S. government, export licenses, business financial assistance, and many other topics.
Internal Revenue Service	http://www.irs.gov/ Home page; access to downloadable IRS forms and publications.
Occupational Safety and Health Administration (OSHA)	http://www.osha.gov/ Home page.
Office of the Comptroller of the Currency (OCC)	http://www.occ.treas.gov/ Home page with links to reports and other resources for banking industry professionals, as well as public information about the national banking system.
Office of Federal Contract Compliance Programs (OFCCP)	http://www.dol.gov/ofccp/index.htm Home page with statutory, regulatory, and compliance information regarding nondiscrimination requirements for federal contractors.
Office of the U.S. Trade Representative	http://www.ustr.gov/index.html Home page.
Securities and Exchange Commission (SEC)	http://www.sec.gov/ Home page with links to information for small businesses; online access to proposed and final rules, SEC releases, policy statements, and other commission notices and information; searchable database of all electronic company filings since 1994.
SEC Edgar	http://www.sec.gov/edgar.shtml SEC Edgar main page, with access to electronic filings and forms.
Small Business Administration	http://www.sba.gov/ Home page with extensive links to federal and other resources for small businesses.
Social Security Administration	http://www.ssa.gov/ Home page. SSA forms are available online at http://www.ssa.gov/online/forms.html
THOMAS	http://thomas.loc.gov/home/thomas.html Website of the Library of Congress providing federal legislative information.
U.S. Citizenship and Immigration Services	http://www.uscis.gov/portal/site/uscis Home page with links to immigration laws and forms.
U.S. Copyright Office	http://www.copyright.gov/ Home page with links to copyright registration and other information. The agency's new Electronic Copyright Office (eCO) is at http://www.copyright.gov/eco/index.html
U.S. Department of Commerce	http://www.commerce.gov/ Home page.
U.S. Department of Justice, Antitrust Division	http://www.usdoj.gov/atr/public/guidelines/guidelin.htm Link to Antitrust Division Guidelines and Policy Statements.
U.S. Department of Labor	http://www.dol.gov/ Home page with links to statutory and regulatory information, labor statistics, small-business regulatory-compliance assistance, and other information.
U.S. Department of	http://www.oalj.dol.gov/libdot.htm

Labor, Dictionary of Occupational Titles (DOT)	Dictionary of job titles and standardized job descriptions; useful for job placement, occupational research, career guidance, labor-market information, curriculum development, and long-range job planning. Last updated in 1991, the DOT has now been replaced by O*NET Online, http://online.onetcenter.org/
U.S. Department of State	http://www.state.gov/ Home page with links to international commercial laws and guides.
U.S. Environmental Protection Agency	http://www.epa.gov/ Home page.
U.S. Government Printing Office	http://www.gpo.gov/ Home page with links to products and services, including online searchable copies of the United States Code and the Code of Federal Regulations.
U.S. International Trade Commission	http://www.usitc.gov/ Home page with rules, regulations, reports, and other information, including an extensive list of links to international trade resources.
U.S. Patent and Trademark Office	http://www.uspto.gov/ Home page with downloadable forms and information on patent applications and trademark registrations.

B. International Sites

Private International Law Database: Trade/Business Transactions Law, U.S. Department of State	http://www.state.gov/www/global/legal_affairs/transaction_law.html Access to treaties in force for the United States, other international instruments, and information on current negotiations and projects concerning private international law. Updated through January 1, 2001. For treaty actions since January 1, 2001, see http://www.state.gov/s/l/treaty/c3428.htm
CURIA	http://curia.europa.eu/jcms/jcms/j_6/ Home page of the courts of the European Communities, with searchable case law and other information.
Electronic Embassy Website	http://www.embassy.org/ Information on all foreign embassies in Washington, D.C.
EUR-Lex	http://eur-lex.europa.eu/en/index.htm Website providing direct free access to European Union law. Among other things, it includes the Official Journal of the European Union, treaties, legislation, case law, and legislative proposals.
European Franchise Federation (EFF)	http://www.eff-franchise.com/ Nonprofit international organization that promotes the interests and development of franchising in Europe.
Hague Conference on Private International Law (HCCH)	http://hcch.e-vision.nl/index_en.php?act=text.display&tid=1 Home page.
International Trademark Association (INTA)	http://www.inta.org INTA is an international nonprofit membership association dedicated to the support and advancement of trademarks and related intellectual property.
NAICS Association	http://www.naics.com/index.html Agency that administers the North American Industry Classification System (NAICS), which replaced the old Standard Industrial Classification (SIC) system in 1997. NAICS codes are used by statistical agencies in the U.S., Canada, and Mexico to classify businesses for the collection, analysis, and

	publication of statistical data related to the economy.
North American Free Trade Agreement (NAFTA) Secretariat	http://www.nafta-sec-alena.org/en/view.aspx Home page with link to text of NAFTA.
Canadian System for Electronic Document Analysis and Retrieval (SEDAR)	http://www.sedar.com/ Home page of the Canadian equivalent to the SEC's EDGAR. Provides access to corporate filings of Canadian companies with Canada's securities regulatory authorities.
United Nations Commission on International Trade Law (UNCITRAL)	http://www.uncitral.org/ Home page with links to UNICITRAL texts, including conventions, model laws, guides to enactment, legislative guides, legislative recommendations, and model contract rules. In particular, this website includes the text of the U.N. Convention on Contracts for the International Sale of Goods (CISG).
CISG Database at Pace University School of Law, Pace Law Library, Institute of International Commercial Law	http://cisgw3.law.pace.edu/ Site dedicated to U.N. Convention on Contracts for the International Sale of Goods (CISG), with annotated text of CISG, CISG in different languages, cases organized by countries, and related CISG material.
International Institute for the Unification of Private Law (UNIDROIT)	http://www.unidroit.org/dynasite.cfm Home page.
World Intellectual Property Organization (WIPO)	http://www.wipo.int/portal/index.html.en A specialized agency of the United Nations, dedicated to developing a balanced and accessible international intellectual property system.
World Trade Organization (WTO)	http://www.wto.org/ Global international organization dealing with the rules of trade between nations.

C. Government Sites—California

California Department of Corporations (DOC), Franchise Regulation	http://www.corp.ca.gov/SRD/franchise.asp Access to information and forms concerning franchise registration.
California Department of Corporations (DOC), Securities Regulation Division	http://www.corp.ca.gov/SRD/default.asp Access to forms, departmental publications, Commissioner's releases, opinions, and notices concerning the California blue sky laws.
Cal-EASI	http://www.corp.ca.gov/CalEASI/caleasi.asp California Department of Corporations website providing access to securities and franchise filings.
California Department of Fair Employment and Housing	http://www.dfeh.ca.gov/ Home page.
California Department of Insurance, Workers'	http://www.dir.ca.gov/workers'_comp.html Access to information on workers' compensation insurance.

Compensation Information	
California Department of Real Estate (DRE)	http://www.dre.ca.gov/ Home page with information for consumers as well as real estate licensees and examinees.
California Division of Occupational Safety and Health (DOSH)	http://www.dir.ca.gov/dosh Access to information concerning the Cal-OSHA program.
California Employment Development Department (EDD)	http://www.edd.ca.gov Home page; information concerning job placement and referrals, unemployment insurance, disability insurance, employment and training, the labor market, payroll taxes, and other topics.
California Franchise Tax Board (FTB)	http://www.ftb.ca.gov/ Home page with links to downloadable state tax forms and publications.
California Law Revision Commission	http://www.clrc.ca.gov/ Home page.
Official California Legislative Information	http://www.leginfo.ca.gov/index.html Full text of bills, resolutions, and constitutional amendments, as well as their status, history, votes, analyses, and veto messages.
California Legislative Resource	http://calbar.ca.gov/state/calbar/calbar_generic.jsp?cid=10137&id=10452 Webpage maintained by the State Bar of California with many helpful links regarding California's legislative process, pending bills, legislative calendar, committees, and other topics.
State Bar of California Bill Tracking Service	http://www.calbar.ca.gov/calbar/legislation/State%20Bar%20Bill%20Tracking-Sections.html Centralized legislative monitoring and tracking service listing bills of potential interest to members of the State Bar's sections and their committees.
CalGOLD	http://www.calgold.ca.gov/ The CalGOLD website provides links and contact information for California businesses concerning business permits, licenses, and registrations required by federal, regional, state, and local agencies. Information is searchable according to type of business.
California Office of Privacy Protection	http://www.oispp.ca.gov/consumer_privacy/default.asp State agency dedicated to promoting and protecting the privacy rights of consumers.
California State Agencies	http://www.ca.gov/ State of California site with links to California agencies, departments, and commissions.
California State Association of Counties	http://www.csac.counties.org/ Home page with links to all California counties.
California State Board of Equalization	http://www.boe.ca.gov/ Home page with access to information about sales and use taxes, sellers' permits, forms, and publications.
California Secretary of State— California Business Portal:	http://www.sos.ca.gov/business/ Home page.
Forms and Fees:	http://www.sos.ca.gov/business/forms.htm

	Directory of forms, sample forms, and fees for different business filings, including UCC forms, some in fill-in format.
Business Filings:	
Business Entities	http://www.sos.ca.gov/business/be/ Business Entities main page with links to services offered for corporations, limited liability companies, limited partnerships, and other business entities; filing tips to meet statutory minimum requirements; name availability; FAQs; and more.
Trademarks and Service Marks	http://www.sos.ca.gov/business/ts/ Trademarks and service marks main page with links to forms and fees, name availability, FAQs, private service companies, and more.
California Business Search	http://kepler.sos.ca.gov Fill-in boxes to check records online for corporations, limited partnerships, and limited liability companies.
Starting a Business	http://www.sos.ca.gov/business/be/starting-a-business.htm A step-by-step guide for starting a business in California.
e-file Statement of Information	https://businessfilings.sos.ca.gov/ Fill-in boxes to file a Statement of Information for a corporation online.
Notary Public	http://www.sos.ca.gov/business/notary/ Notary public main page, with links to topics such as obtaining a notary public commission, handbook, authentications, apostille or certification, forms, and fees.
Uniform Commercial Code	http://www.sos.ca.gov/business/ucc/ UCC main page with links to UCC Connect (the Secretary of State's online service for UCC inquiries, filings, requests for copies and debtor search certificates, and more), financing statement forms and filing fees, administrative rules, FAQs, and other resources.
International Business Relations Program	http://www.sos.ca.gov/business/ibrp/ Main page with links to chambers of commerce, foreign consulates, trade associations, and other agencies, and to other resources to assist foreign business entities with various California filing procedures.
Business Program Division, Legislation	http://www.sos.ca.gov/business/bpd_newleg.htm Summaries and links to new state laws affecting businesses.
Victims of Corporate Fraud Compensation Fund	http://www.sos.ca.gov/vcfcf/ Main page with information, including application requirements, instructions, and forms, concerning the fraud compensation fund administered by the Secretary of State's office.

D. Private Agency Sites

ABA Section of Business Law	http://www.abanet.org/buslaw/home.html Home page with links to publications and other resources for business lawyers.
Active Capital	http://activecapital.org/ Site dedicated to helping individual accredited investors, SBICs, and institutional venture capitalists find small, growing companies through a secure Internet database, and providing ongoing training and research for entrepreneurs and small investors.
AllBusiness	http://www.allbusiness.com Small business portal, with links to forms, directories, and resources on many

	topics.
American Arbitration Association	http://www.adr.org/ Home page with links to rules and procedures.
American Intellectual Property Law Association (AIPLA)	http://www.aipla.org Home page with links to practice areas, professional development, educational materials, meetings, and events.
Annual Reports.com	http://www.annualreports.com/ Free service offering links to annual reports of public companies.
BenefitsLink	http://www.benefitslink.com Compliance information and tools for employee benefit plan sponsors, service providers, and participants.
Better Business Bureau	http://www.bbb.org/ National home page. There are separate regional Better Business Bureaus covering different geographical areas of California, each with its own website.
The Biz-Tech Network by Brint Institute, LLC	http://www.brint.com/ Portal with a meta-index of business, management, and information technology topics; it also provides search capabilities and full text articles on related issues.
Business.com	http://www.business.com/ Business search engine and directory intended to help users find companies, products, services, and other business-related information; some features are fee-based.
Business Law Section of the State Bar of California	http://www.calbar.ca.gov/state/calbar/calbar_sections_generic.jsp?sCategoryPath=/Home/Attorney%20Resources/Sections/Business%20Law Home page with links to standing committees, programs, and publications.
Business Week Online	http://www.businessweek.com/ Articles, links, and opportunity to subscribe to free newsletter.
CNBC	http://www.cnbc.com/ Home page of business and financial news cable network.
CNN Money	http://money.cnn.com/?cnn=yes General business news website offered by CNN and *Fortune* and *Money* magazines.
Corporate Finance Sourcebook	http://www.financesourcebook.com/ Link for ordering popular guidebook published by National Register Publishing. The guidebook features over 1500 top investment sources and 1700 service firms for business entrepreneurs.
Corporate Information	http://www.corporateinformation.com/ Subscription-based website offering research reports on public, private, domestic, and foreign corporations.
The Corporate Library	http://www.thecorporatelibrary.com/ The Corporate Library is an independent research firm providing corporate governance data, analysis, and risk assessment tools.
Creative Commons	http://creativecommons.org A nonprofit organization founded by Prof. Lawrence Lessig of Stanford University that provides special copyright license forms and other free tools to enable authors, scientists, artists, and educators to share intellectual property.

Dun & Bradstreet	http://www.dnb.com/us/ Home page of Dun & Bradstreet. Subscribers can request reports and run online queries in proprietary databases.
Edgar Online, Inc.	http://www.edgar-online.com/ Edgar Online, Inc. is a private company, not affiliated with the SEC, specializing in the extraction, packaging, and distribution of public-company information contained in SEC filings.
Entrepreneur.com	http://www.entrepreneur.com/mag Free access to *Entrepreneur* magazine articles back to 1998.
Financial Accounting Standards Board (FASB)	http://www.fasb.org/ Access to FASB Statements of Financial Accounting Standards and other resources.
Findlaw Business Center	http://smallbusiness.findlaw.com/ Portal with links to articles and guides on starting a business, taxes and accounting, small business legal concerns, and more. Part of West Group.
Garage Technology Ventures	http://www.garage.com/ Venture capital fund for emerging technology companies.
GNU	http://www.gnu.org/ Organization promulgating the development and use of free software and the use of open-source software licenses.
Google Business News	http://news.google.com/nwshp?tab=wn&ned=us&topic=b Business news headlines with links to full stories from news organizations around the world.
Google Small Business Directory	http://directory.google.com/Top/Business/Small_Business/ A directory of small business resources.
Hieros Gamos Small Business Center	http://www.hg.org/sbcenter.html Portal with links to topics such as starting a business, choosing a legal structure, and financing.
Hoover's Online	http://www.hoovers.com/ Subscription-based site with industry snapshots, company profiles, earnings, and other information.
Intellectual Property Law Section of the State Bar of California	http://www.calbar.ca.gov/state/calbar/calbar_sections_generic.jsp?cid=10707 Home page with links to standing committees, programs, and publications.
International Franchise Association (IFA)	http://www.franchise.org/ Trade association promoting responsible franchise development worldwide.
Internet Corporation for Assigned Names and Numbers (ICANN)	http://www.icann.org/ Private agency responsible for global coordination of the Internet's system of unique identifiers, including domain names (such as .com, .org, and country codes such as .fr), as well as addresses used in a variety of Internet protocols.
IP Mall	http://ipmall.info/ Website sponsored by Franklin Pierce Law Center, with links to intellectual property resources around the world (including patents, copyrights, trademarks, trade secrets, licensing, and technology transfers).
JAMS	http://www.jamsadr.com

	Home page with information about JAMS mediation and arbitration services and a search engine to assist in locating qualified mediators and arbitrators. The website also offers sample dispute resolution clauses for commercial contracts.
Jefren Publishing Co.	http://www.jefren.com Subscription service offering proxy statement forms and strategies.
MarketResearch.com	http://www.marketresearch.com/ Free database of market research reports representing all market and industry sectors.
NASDAQ	http://www.nasdaq.com/ Comprehensive current information on market performance and investments.
National Association of Attorneys General	http://www.naag.org/ Association of the attorneys general of all 50 states, with contact information and links to enforcement initiatives.
National Association of Seed and Venture Funds	http://www.nasvf.org/ Network of private, public, and nonprofit organizations investing and facilitating investment in entrepreneurs.
National Business Association	http://www.nationalbusiness.org/ Nonprofit association's site for the self-employed and small business community.
National Venture Capital Association (NVCA)	http://www.nvca.org/ Home page with links to members and other resources.
New York Stock Exchange (now NYSE Euronext)	http://www.nyse.com/ Comprehensive, current information on market performance and investments.
PayChex	http://www.paychex.com/index.aspx Company offering payroll processing, human resources administration and compliance, and employee benefit administration services for small and mid-sized businesses.
PayPal Merchant Services	https://merchant.paypal.com/cgi-bin/marketingweb?cmd=_render-content&content_ID=merchant/home Commercial service enabling businesses to accept credit card and other payments securely on websites, by e-mail, or over the telephone.
The Public Register Online	http://www.annualreportservice.com/ Free access to annual reports of over 2200 companies. Site also has links to the SEC's Edgar database for filings.
Reuters	http://www.reuters.com/finance Business and finance news database with reports on business transactions, markets, small businesses, industries, the economy, and other topics.
Safeselling.org	http://www.safeselling.org/ ABA-sponsored resource for business people launching e-commerce enterprises and for businesses venturing into online sales.
The Small Business Portal	http://www.thesmallbusinessportal.com/ Links to topics such as starting a business, franchise advice, financing, and home-based businesses.
Standard & Poor's	http://www.standardandpoors.com/ Home page with search engine for public company credit ratings and other

	features.
Tripod by Lycos	http://www.tripod.lycos.com/smallbiz/index.html Portal with tips on starting an online business, yellow pages, and some free and some fee-based services.
U.S. GAAP Information	http://cpaclass.com/gaap/ Comprehensive source of information on generally accepted accounting principles in the U.S.
Wall Street Journal Online Edition	http://online.wsj.com/home-page General business and financial news.
Washburn University School of Law Small Business Portal	http://www.washlaw.edu/subject/small.business.html Portal with links to a forms library and business and economic data.
Yahoo! Finance	http://biz.yahoo.com/i/ Free company profiles and stock charts for over 9000 public companies.
Yahoo! Small Business	http://smallbusiness.yahoo.com/index.html? Portal with links to topics such as creating a website, promoting a business, and selling online.

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/Table of Statutes, Regulations,and Rules

Table of Statutes, Regulations,and Rules

CALIFORNIA

Constitution

Art I, §1: §9.16

Art XV §1: §16.22

Statutes

BUSINESS AND PROFESSIONS CODE

44-1372: §17.24

300-313.5: §17.9

407.1123: §17.24

6157-6159.2: §§17.9, 17.10B

14200-14272: §§3.5, 3.26, 3.31, 20.1

14202(h): §3.31

14207: §3.31

14215(b): §3.31

14217(a)-(b): §3.31

14220: §§5.1, 16.29

14230: §3.31

14260: §5.1

14411-14418: §3.27

16600: §§2.26, 4.11

16601: §4.11

16601-16602.5: §2.26

17200: §§9.27, 17.9, 20.7

17200-17210: §§9.18, 9.27

17201: §17.9

17204: §17.9

17206: §17.9

17500: §§17.8-17.9

17508(f): §17.9

17510-17510.95: §17.9

17511-17513: §17.9

17525: §§3.22, 20.32

17525-17528: §§3.22, 17.8, 20.1, 20.32

17526(d): §20.32

17529-17529.9: §17.24

17529.1(o): §§17.25-17.26

17529.2: §§17.25-17.26

17529.4: §17.26

17529.4(a): §17.25

17529.4(b): §17.25

17529.5: §§17.25-17.26

17529.5(a)(1): §17.25

17529.5(a)(2): §17.25

17529.5(a)(3): §17.25

17529.8: §17.25

17538: §§17.8, 17.10

17538(a): §17.10

17538(d): §17.10

17538(d)(1): §17.10

17538(d)(2): §17.10

17538(g): §17.10

17538.45: §§17.24, 17.26

17538.45(c): §17.25

17538.45(f): §17.25

17539-17539.6: §17.9

17900-17930: §3.27

22575-22579: §§9.1-9.2, 9.18-9.19, 9.21, 9.39, 9.43, 9.45

22575(a): §§9.19, 9.21, 9.39

22575(b)(1)-(4): §9.20

22576: §§9.19, 9.21

22576(a)-(b): §9.21

22577(a)(1)-(7): §9.19

22577(b)(1)-(5): §§9.19, 9.41

22947-22947.6: §§9.6B, 9.18, 9.26A, 9.27

22947.1(b): §9.26A

22947.2-22947.3: §9.26A

22947.3(d): §9.26A

22947.4: §9.26A

22948-22948.3: §§3.63, 9.6C, 9.18

22948.2: §3.63

22948.3(a)(1): §§3.63, 9.6C

22948.3(a)(2): §9.6C

22948.6: §18.16A

22948.6(a)(1)-(2): §18.16A

CIVIL CODE

44: §20.2

44-45: §20.2

45: §§20.2-20.3

45-46: §20.2

46: §20.2

47: §20.2

48a: §20.2

48a(4)(b): §20.2

51-53: §5.26

54-55.2: §5.26

56-56.37: §9.18

980: §4.7

985: §9.18

1301: §19.19

1624: §5.1

1633.1-1633.17: §§7.1, 7.9, 10.2

1633.5(a): §7.10

1633.5(b): §7.10

1646: §§19.16, 19.19

1646.5: §§19.19-19.20

1654: §4.2

1708.8: §9.21A

1708.8(a)-(b): §9.21A

1708.8(d)-(e): §9.21A

1708.8(f): §9.21A

1739.7: §20.7

1750-1784: §17.9

1770(a)(2): §17.9

1770(a)(9): §17.9

1770(a)(13): §17.9

1770(a)(14): §17.9

1770(a)(18): §17.9

1785.1-1785.43: §9.18

1786-1786.56: §9.18

1798-1798.78: §9.18

1798.29: §§9.18, 9.24

1798.81.5: §§9.18, 9.25, 18.15

1798.82: §§18.15, 18.23

1798.82-1798.84: §§9.18, 9.24-9.25

1798.82(a): §§9.24, 18.15

1798.82(b): §18.15

1798.82(e): §§9.24-9.25, 18.15

1798.82(f)(1): §18.15

1798.82(f)(2): §18.15

1798.82(f)(3): §18.15

1798.82(g): §9.24

1798.82(g)(1)-(2): §18.15

1798.82(g)(3): §§9.24, 18.15

1798.83: §§9.18, 9.26

1798.83(a): §9.26

1798.83(b): §9.26

1798.83(c)(2): §9.26

1798.83(d): §9.26

1798.83(e)(7): §9.26

1798.84(a): §18.15

1798.84(b): §18.15

1798.84(e): §18.15

1798.91: §9.18

1916.1: §16.22

3344: §§9.18, 20.9

3425.1-3425.5: §20.2

3426-3426.11: §§2.20, 2.34, 4.6, 20.1

3426.1(d): §§2.21, 2.27, 4.6

3426.2(a): §2.34

3426.3: §2.36

3426.3(c): §2.36

3426.4: §2.36

3426.5: §2.37

CODE OF CIVIL PROCEDURE

410.10: §§19.2-19.3

410.40: §19.12

425.16: §§20.1, 20.3, 20.25

425.16(b)(1): §20.25

425.16(d): §20.25

425.16(e): §20.25

425.16(f): §20.25

426.16: §20.25

1985.8(b): §§20A.18D, 20A.27

1985.8(c)(1): §§20A.18D, 20A.40

1985.8(c)(2): §20A.18D

1985.8(d)-(e): §20A.18A

1985.8(f): §20A.18A

1985.8(h): §20A.18E

1985.8(h)(4): §20A.3

1985.8(i): §§20A.18C, 20A.44

2016.010-2036.050: §20A.18

2016.020(d)-(e): §20A.18

2017.010: §20A.29

2025.230: §20A.30

2031(g) (former): §20A.49

2031(g)(1) (former): §20A.49

2031.010: §20A.38

2031.010(a): §20A.18

2031.030(a)(2): §20A.18D

2031.060(c)-(e): §20A.18A

2031.060(e): §20A.18A

2031.060(i): §20A.18B

2031.210(d): §20A.18A

2031.280(a): §20A.43

2031.280(c): §20A.49

2031.280(d): §20A.27

2031.280(d)(1): §§20A.18D, 20A.40

2031.280(d)(2): §20A.18D

2031.285: §§20A.18C, 20A.44

2031.285(a): §20A.18C

2031.285(b): §20A.18C

2031.285(c)(2): §20A.18C

2031.285(d)(1): §20A.18C

2031.285(d)(2): §20A.18C

2031.300(d)(1): §20A.18B

2031.310(d)-(e): §20A.18A

2031.310(f): §20A.18A

2031.310(g): §20A.18E

2031.320(d)(1): §20A.18B

COMMERCIAL CODE

1105(2): §19.19

1201: §7.6

1301(a): §§19.19-19.20

1301(c): §19.19

9101-9709: §16.26

9102(a)(42): §§16.26, 16.30-16.31

9109(c)(1): §16.26

9203(b): §16.26

9307: §16.26

9310: §16.26

9310(a): §16.31

9317: §16.26

9322: §16.26

9501: §16.26

CORPORATIONS CODE

400-403: §16.2

25019: §16.34

25102(f): §16.22

25102(f)(2): §16.22

25116(a): §16.22

25118(a): §16.22

25118(b): §16.22

25118(f)-(g): §16.22

EDUCATION CODE

18030.5: §20.21

32261(d): §20.22A

32261(g): §20.22A

32265(b)(9): §20.22A

48900(r): §20.22A

67140-67147.5: §9.18

EVIDENCE CODE

1060: §2.37

FAMILY CODE

6700-6710: §7.3

FINANCIAL CODE

1716: §16.22

4050-4060: §§9.18, 9.22

4051.5(a)(4): §9.22

4052.5: §9.22

4053: §9.22

4053(a): §9.22

4053(a)(2): §9.22

22002: §16.22

GOVERNMENT CODE

7460-7493: §§9.18, 9.23

7465(a): §9.23

7470(a)(1)-(4): §9.23

7471-7476: §9.23

7480: §9.23

LABOR CODE

510: §4.12

515: §4.12

515.5: §4.12

515.5(a)(1): §4.12

515.5(a)(2): §4.12

515.5(a)(3): §4.12

515.5(a)(4): §4.12

515.5(b)(3): §4.12

515.5(b)(5): §4.12

515.5(b)(6): §4.12

515.6: §4.12

2860: §4.9

2870: §§4.11, 5.12

2870(a): §§4.9-4.10

2870(b): §4.10

2872: §4.11

2922: §4.3

PENAL CODE

311-311.11: §20.13

313-313.5: §20.22

313(a): §20.22

313.1: §20.22

313.4: §20.22

350: §3.61

350(i): §3.61

502: §18.16

502(b)(8): §18.16

502(b)(10): §18.16

502(c): §§17.27, 18.16

502(c)(3): §17.27

502(c)(9): §17.27

502(d): §18.16

502(d)(2): §17.27

502(d)(5): §17.27

502(e)(1): §§17.27, 18.16

630-637.6: §9.18

653aa: §8.26A

653aa(a): §8.26A

653aa(b): §8.26A

653aa(c): §8.26A

653.2: §20.12

653.2(a): §20.22

653.2(c)(1): §20.22

REVENUE AND TAXATION CODE

6001-7176: §10.24

6001-7226: §10.22

6051: §10.24

6201: §10.24

6202-6203: §10.24

6203(c): §10.24

6203(c)(4): §10.24

6203(d)(1): §10.24

6292-6293: §10.24

65001-65004: §10.21

ACTS BY POPULAR NAME

Anti-Phishing Act of 2005: §§3.63, 9.6C, 9.18

California Consumers Legal Remedies Act: §17.9

California Financial Information Privacy Act: §§9.18, 9.22-9.23

California Internet Tax Freedom Act (California ITFA): §§10.21, 10.24

California Invasion of Privacy Act: §9.18

California Online Privacy Protection Act of 2003: §§9.1-9.2, 9.18-9.19, 9.21, 9.39, 9.43, 9.45

California Right to Financial Privacy Act: §§9.18, 9.23

Civil Discovery Act: §20A.18

Confidentiality of Medical Information Act: §9.18

Consumer Credit Reporting Agencies Act: §9.18

Consumer Protection Against Computer Spyware Act: §§9.6B, 9.18, 9.26A, 9.27

Disabled Persons Act: §5.26

Electronic Discovery Act: §§20A.3, 20A.18-20A.18A, 20A.18C, 20A.38, 20A.40, 20A.44

Information Practices Act of 1977: §9.18

Investigative Consumer Reporting Agencies Act: §9.18

Model State Trademark Act: §3.31

State Bar Act

Art 9.5: §17.10B

Unfair Competition Law: §9.18

Uniform Electronic Transactions Act (UETA): §§7.1, 7.9-7.10, 7.14, 10.2

Uniform Trade Secrets Act (UTSA): §§2.34, 4.6, 20.1

Unruh Civil Rights Act: §5.26

SESSION LAWS

Stats 2009, ch 5: §§20A.3, 20A.18

Stats 2001, ch 343: §10.21

Stats 1998, ch 599: §17.8

PROPOSED LEGISLATION

SB 394: §10.21

SB 186: §17.25

AB 1791: §10.21

Regulations

CALIFORNIA CODE OF REGULATIONS

Title 10

260.102.14: §16.22

Title 18

1502: §10.25

1502(f)(1): §10.25

1502(f)(1)(B): §10.25

1502(f)(1)(C): §10.25

1502(f)(2)(A): §10.25

Title 22

4304-1: §4.14

Rules

CALIFORNIA RULES OF COURT

2.550-2.551: §2.37

3.724(8): §§20A.17, 20A.39

3.724(8)(E): §20A.17

CALIFORNIA RULES OF PROFESSIONAL CONDUCT

1-400: §17.10B

1-400(A): §17.10B

1-400(C): §17.10B

1-400(F): §17.10B

3-310: §4.2

3-600: §5.5

Ethics Opinions

STATE BAR OF CALIFORNIA

2005-168: §17.10B

2004-166: §17.10B

2001-155: §17.10B

UNITED STATES

Constitution

Art I, §8: §1.1

Art I, §8, cl 8: §2.2

Art III, §2: §19.1

Amend I: §§1.3, 1.28, 17.11, 17.13, 17.28, 20.1, 20.3, 20.9, 20.14-20.17, 20.23-20.24, 20.28, 21.5

Amend IV: §§9.7, 9.15

Amend V: §§1.28, 19.3

Amend XIV: §§17.11, 19.3, 19.15, 20.15

Statutes

UNITED STATES CODE

Title 7

181-229b: §17.4

Title 11

365: §12.13

365(a): §12.12

365(b)(1): §12.12

365(e): §12.13

365(n): §§12.12-12.13, 15.2

365(n)(1)(A): §12.12

365(n)(1)(B): §12.12

365(n)(4): §12.12

365(n)(4)(A): §12.12

541(a)(1): §12.12

Title 12

3401-3422: §9.13

3402: §9.13

3404-3408: §9.13

3404(b): §9.13

3412: §9.13

Title 15

41-58: §§17.2, 17.4, 17.11, 20.1

41-77: §17.22

45: §§17.4, 17.7A

45(a): §9.9

45(a)(2): §17.4

45(a)(3): §17.4

45(b): §17.6

45(c): §17.6

45(l): §17.6

45(l)-(m): §17.6

45(m)(1)(A): §9.33

53: §17.6

53-54: §17.6

54: §17.6

57a(a)(1)(B): §17.22

57b: §17.6

57b(b): §17.6

77a-77aa: §16.34

764.3(b)(1)-(2): §21.25

1015(b): §3.42

1051: §3.34

1051-1052: §3.47

1051-1141n: §§3.26, 3.71, 16.29, 17.2-17.3, 20.1

1051(a): §3.42

1051(a)(1): §§3.38-3.39

1051(a)(2): §§3.38-3.39, 3.43

1051(a)(3): §3.40

1051(a)(3)(C): §3.34

1051(a)(3)(D): §§3.38, 3.40

1051(b): §§3.35, 3.42, 3.49

1051(b)(2): §§3.39, 3.43

1051(c)-(d): §3.35

1051(d): §§3.35, 3.57

1052: §§3.32, 3.34

1052(a): §3.32

1052(a)-(e): §3.32

1052(d): §§3.29, 3.40

1052(e)(1): §3.28

1052(e)(2): §3.32

1052(e)(3): §3.32

1052(f): §§3.28-3.29

1053: §3.27

1057(b): §3.30

1057(c): §§3.30, 3.35

1058(a): §3.52

1058(b): §3.52

1058(c): §3.52

1060: §§3.57, 5.1, 16.29-16.30

1060(a): §5.1

1060(a)(3): §3.57

1060(a)(4): §3.57

1063: §3.49

1064: §3.49

1064(1): §3.49

1064(3): §3.49

1065: §3.30

1070: §3.50

1072: §§3.30, 3.34

1091: §3.34

1091(a): §3.28

1111: §§3.30, 3.34, 3.51

1112: §3.41

1114: §§3.60, 20.29

1114(1): §§3.4, 3.71

1115(a): §3.34

1115(b)(4): §3.64

1116: §3.63

1117: §§3.24, 3.30

1117(a): §3.63

1121: §3.60

1121(a): §§3.30, 3.34

1124: §§3.30, 3.34

1125: §§3.65, 3.68, 20.29

1125(a): §§3.51, 3.61, 3.84, 18.19

1125(a)(1): §§3.67, 17.3

1125(a)(3): §§3.77-3.78

1125(c): §§3.22, 3.65

1125(c)(1): §§3.23, 3.65

1125(c)(2): §§3.65-3.66

1125(c)(2)(A): §3.66

1125(c)(2)(B): §3.65

1125(c)(2)(C): §3.65

1125(c)(3): §20.29

1125(c)(3)(A): §3.68

1125(c)(3)(C): §20.29

1125(c)(5)(B)(ii): §3.68

1125(d): §§3.11, 3.22, 3.62, 19.11, 20.1, 20.31

1125(d)(1)(A): §§3.23-3.24

1125(d)(1)(B): §3.23

1125(d)(1)(B)(ii): §3.23

1125(d)(1)(C): §3.24

1125(d)(2): §19.11

1125(d)(2)(A)(ii): §3.22

1125(d)(2)(A)(ii)(II): §3.22

1125(d)(2)(A)(ii)(II)(aa): §3.22

1125(d)(2)(D): §3.24

1126(d): §3.42

1126(e): §3.42

1127: §§3.27, 3.34, 3.47, 3.53

1129: §§20.1, 20.31

1129(a)(1)(A): §3.22

1141-1141n: §3.48

1681-1681x: §9.9A

1691a(d): §9.9A

1691a(e): §9.9A

6501-6506: §§9.28-9.29, 9.40, 20.20

6501(1): §9.29

6501(8): §9.31

6501(8)(G): §9.31

6501(10)(A)(ii): §9.30

6502(a): §9.30

6502(b): §9.31

6502(b)(2)(A): §9.34

6502(b)(2)(B): §9.34

6502(b)(2)(C): §9.34

6502(b)(2)(D): §9.34

6502(b)(2)(E): §9.34

6801-6809: §9.12

6801-6827: §9.12

6804: §9.12

6805(a): §9.12

7001-7006: §10.2

7001-7031: §§7.1, 7.5

7001(a)(1): §7.5

7001(a)(2): §7.5

7001(b)(2): §§7.5, 7.10

7001(c): §7.7

7001(c)(1)(A): §7.7

7001(c)(1)(B)(i): §7.7

7001(c)(1)(B)(ii): §7.7

7001(c)(1)(B)(iii): §7.7

7001(c)(1)(B)(iv): §7.7

7001(c)(1)(C)(i): §7.7

7001(c)(1)(C)(ii): §7.7

7001(c)(1)(D)(i): §7.7

7001(d)(1): §7.8

7001(e): §7.8

7002: §7.9

7006(5): §§7.5-7.6

7021: §10.2

7031: §10.2

7701-7713: §§17.11-17.12, 18.4, 20.1

7702(1): §17.20

7702(1)(A): §17.18

7702(1)(B): §17.18

7702(2)(A): §17.13

7702(2)(B): §17.13

7702(2)(D): §17.13

7702(16)(B): §17.21

7702(17)(A): §17.13

7702(17)(B): §17.13

7704(a): §17.19

7704(a)(1): §17.15

7704(a)(1)-(2): §17.15

7704(a)(3)(B): §17.16

7704(a)(3)(C): §17.16

7704(a)(4)(A): §17.16

7704(a)(4)(B): §17.18

7704(a)(5): §§17.14-17.16

7704(b): §17.19

7704(c): §17.19

7704(d): §17.20

7704(d)(1)(B): §17.20

7704(d)(2): §17.18

7704(d)(5): §17.20

7705: §17.21

7706: §17.22

7706(f): §17.22

7706(g): §17.22

7707(b)(1): §17.26

7707(b)(2): §17.26

7707(c): §17.26

7708: §17.23

7709: §17.12

7711: §17.12

7711(b): §17.15

7712(b): §17.23A

Title 17

101: §§1.2-1.6A, 1.9, 4.8, 5.12, 8.26, 16.27

101-1332: §§1.1, 20.1

102: §§1.2, 2.22A

102(a): §§1.7, 14.3

102(b): §§1.2, 14.3

103: §1.2

103(b): §1.2

104A: §1.3

105: §14.5

106: §§1.6A, 1.9, 1.12, 6.9, 14.1, 14.17

106(1): §§1.6, 14.4

106(2): §§1.6, 14.4

106(3): §§1.6, 1.6B, 14.4

106(4): §§1.6, 14.4

106(5): §§1.6, 14.4

106(6): §8.25

107: §§1.18-1.19, 14.1, 14.6

107-121: §1.6

107(1): §1.19

107(2): §1.20

107(3): §1.21

107(4): §1.22

109: §§1.3, 1.6, 1.23

109(a): §1.23

109(b): §1.23

111: §8.25

112(a)(1): §8.27

114: §14.17

114-115: §8.25

114(d)-(f): §8.25

114(d)(1): §8.25

114(d)(1)(A): §8.27

114(d)(2)-(j): §8.25

114(e)-(f): §8.25

114(f): §8.25

114(h): §8.25

117: §§1.6A, 1.16B, 1.23

117(a): §1.16B

117(c): §1.16B

119: §8.25

201: §1.4

201(a): §§1.5, 4.18, 5.6

201(b): §§1.5, 4.8, 4.18

201(d): §1.9

203: §1.9

204: §§1.9, 5.1

204(a): §1.9

204(b): §1.9

205: §§5.1, 16.27

205(a): §1.9

205(c): §§1.9, 16.27

205(d): §1.9

205(e): §1.9

261: §2.15

302: §1.3

401: §1.7

401(a): §1.7

401(b): §1.7

401(c): §1.7

401(d): §1.7

407(a)(1): §1.8A

408(a): §§1.7-1.8

408(f): §1.8C

408(f)(3): §1.8C

410(c): §1.8

410(d): §1.8A

411: §§1.8A-1.8B

411(a): §§1.8, 1.8C

412: §1.8

501: §§1.12-1.13

501-513: §8.23

502: §1.17

503: §1.17

504: §§1.7, 1.17, 8.26

504(c): §§1.8, 1.27

504(c)(2): §1.7

505: §1.17

506: §18.14

506(a): §§1.17, 8.26

506(a)(1)(B)-(C): §8.26B

506(a)(1)(C): §8.26B

506(b): §1.17

507(a): §8.26

512: §§1.24, 1.29, 8.2, 8.25, 18.13

512(a): §1.31

512(a)-(d): §§1.29, 1.42

512(a)(1)-(5): §1.31

512(b): §§1.19, 1.32

512(b)(1): §1.32

512(b)(1)(B): §1.32

512(b)(2): §1.32

512(b)(2)(A): §1.32

512(c): §§1.33-1.37, 8.2

512(c)(1)(A): §1.33

512(c)(1)(B): §§1.33, 1.35

512(c)(1)(C): §§1.33, 1.36

512(c)(2): §1.34

512(c)(3): §§1.33-1.34, 1.37

512(c)(3)(A): §§1.36-1.37, 1.41

512(c)(3)(B)(i): §1.37

512(d): §§1.40, 8.2

512(d)(1)-(3): §1.40

512(d)(3): §1.40

512(f): §1.37

512(g): §1.40

512(g)(1): §§1.36, 1.38

512(g)(1)-(2): §1.38

512(g)(2): §1.38

512(g)(2)-(3): §1.37

512(g)(2)(A): §1.36

512(g)(2)(B): §1.38

512(g)(2)(C): §1.38

512(g)(3): §§1.36, 1.38

512(h): §§1.29, 1.41-1.42

512(h)(1): §1.41

512(h)(2): §1.41

512(h)(3): §1.41

512(h)(4): §1.41

512(h)(5): §1.41

512(h)(6): §1.41

512(i): §§1.30-1.31

512(k)(1)(A): §1.30

512(k)(1)(B): §1.30

512(n): §1.29

801-803: §8.25

1001-1010: §8.24

1001(3): §8.24

1002: §8.24

1003-1005: §8.24

1003(b)-(c): §8.24

1006-1007: §8.24

1008: §8.24

1009: §8.24

1201: §§1.25-1.27

1201-1205: §§1.24-1.25, 8.25, 18.13-18.14, 20.1

1201-1332: §8.2

1201(a): §§1.25-1.26

1201(a)(1): §1.26

1201(a)(1)(A): §1.25

1201(a)(1)(B)-(C): §1.26

1201(a)(2): §1.25

1201(a)(3)(A): §1.25

1201(b): §§1.25, 1.28

1201(b)(1)(A): §§1.25, 1.28

1201(b)(1)(C): §1.28

1201(c): §1.25

1201(c)(3): §1.25

1201(d): §1.26

1201(e): §1.26

1201(f): §1.26

1201(f)(3): §1.26

1201(g): §1.26

1201(h): §1.26

1201(i): §1.26

1201(j): §1.26

1201(k): §1.25

1202(b): §1.25A

1202(c): §1.25A

1203(c): §1.27

1203(c)(2): §1.27

1203(c)(3)(A): §1.27

1203(c)(5)(A): §1.27

1203(c)(5)(B): §1.27

1301-1332: §§1.24, 8.25, 18.13

Title 18

497: §18.14

875: §18.14

1029: §18.14

1030: §§9.14, 17.28, 18.3-18.7, 18.9-18.10, 18.12, 18.19, 20.1, 20.38

1030(a): §§9.14, 18.3-18.4, 18.7A

1030(a)-(c): §17.28

1030(a)(2): §18.7A

1030(a)(2)(C): §§18.4-18.5, 18.7

1030(a)(4): §§18.5, 18.7A

1030(a)(5): §§18.6, 18.7A

1030(a)(5)(A)(i): §18.6

1030(a)(5)(B)(i): §18.12

1030(c): §18.12

1030(c)(2)(B)(ii): §18.5

1030(c)(4)(A): §18.3

1030(e)(2)(b): §18.12

1030(e)(6): §18.5

1030(e)(8): §§18.3, 18.6-18.7

1030(e)(8)(A): §18.4

1030(e)(10): §18.12

1030(g): §§9.14, 17.28, 18.3

1037: §§17.12, 17.19, 18.4

1037(a): §17.23B

1037(b): §17.23B

1037(c): §17.23B

1037(d)(3): §17.23B

1341: §18.14

1343: §18.14

1362: §18.14

1460-1466: §20.16

1465: §§20.13, 20.16

1831: §2.38

1831-1839: §§2.38, 18.14

1831(a): §2.38

1832: §2.38

1961-1968: §20.12

1962(c): §20.12

2251: §§20.13, 20.19

2251-2260: §§20.13, 20.19

2251(a): §20.19

2251A: §20.19

2252-2252A: §20.19

2252(a): §§20.13, 20.19

2252(b): §20.19

2252A: §20.13

2252A(c): §20.13

2252A(c)-(d): §20.19

2252A(d): §20.19

2252B: §3.2

2252B(a): §20.16

2252B(a)-(b): §3.2

2256(1): §20.19

2256(2): §20.19

2256(8)(B): §20.19

2256(8)(D): §20.19

2258A-2258D: §20.13

2258A(a): §20.13

2258A(b): §20.13

2258A(b)(e): §20.13

2258B: §20.13

2260(a): §20.19

2260(b): §20.19

2260(c): §20.19

2261A: §18.14

2311: §8.26

2318-2319: §18.14

2319: §1.17

2319(c): §8.26

2319(d)(1): §8.26B

2319(d)(1)-(2): §8.26B

2319(d)(3): §8.26B

2319(d)(3)-(4): §8.26B

2319A-2319B: §18.14

2320: §18.14

2510: §18.14

2510-2522: §§9.15, 18.6, 18.7A, 18.8-18.10, 18.11A, 20.1

2510(4): §§18.8, 18.11A

2510(17): §18.11

2511: §§18.8, 18.11A

2511(1)(a): §§9.15, 18.8

2511(1)(b): §18.11A

2511(2)(d): §18.9

2512: §18.14

2520: §§9.15, 18.8

2701: §18.14

2701-2712: §§9.15, 18.6, 18.7A, 18.8-18.9, 18.11-18.11A, 20.1, 20A.5

2701(a)(1): §18.11

2701(c): §18.11

2701(c)(1): §9.15

2701(c)(2): §§18.9, 18.11

2702(b)(6): §20.13

2707(a): §18.11

2710: §9.8

3103a(b): §18.12

3121: §§18.11A, 18.14

3121-3127: §18.11A

3127(3): §18.11A

Title 20

1232g: §9.8

9134: §20.21

Title 28

1331: §19.1

1332: §19.1

2461: §17.6

Title 35

9-10: §2.22A

100-376: §2.2

101: §§2.3, 2.7-2.8, 2.19

102: §§2.9, 2.13

102(a): §2.8

102(b): §§2.8, 2.13

102(d): §2.8

102(e): §2.8

102(f): §2.6

102(g): §2.8

103(a): §2.9

111: §2.22A

111(a)(1): §2.10

111(a)(2): §2.10

112: §§2.11-2.12

113: §2.10

115: §2.10

116: §2.6

131: §2.10

134: §2.10

141: §2.10

154(a): §2.2

154(a)(2): §§2.4, 2.22A

161: §2.3

171: §2.3

173: §2.4

261: §§2.15, 5.1, 16.28

262: §2.6

271(b): §2.2

284: §2.2

287(a): §2.10

Title 42

2000aa: §18.14

12101-12213: §5.26

17611-17617: §20.13

Title 47

151: §10.20

222: §9.8

223: §§18.14, 20.18

223(a): §§20.5, 20.18

223(d): §20.5

230: §§20.1, 20.4-20.6D, 20.6C, 20.7

230(c)(1): §§20.5, 20.28

230(c)(2): §20.5, 20.6D

230(e)(2): §§20.6C, 20.16

230(e)(3): §20.7

230(f)(3): §20.5

231: §§10.2, 20.20

231(a)(1): §20.20

231(e)(6): §20.20

254: §20.21

551: §9.8

553: §18.14

605: §18.14

Title 50

1701-1707: §21.25

1705(c): §21.25

2006 Amendment Advisory Committee Note

26: §20A.11

26(f): §20A.11

34: §§20A.13-20A.14

37: §20A.15

INTERNAL REVENUE CODE

3509: §4.13

4251: §10.20

ACTS BY POPULAR NAME

Americans with Disabilities Act of 1990 (ADA): §5.26

Anti-Dilution Act: §§3.22, 3.65, 3.67

Anticybersquatting Consumer Protection Act (ACPA): §§3.1, 3.11, 3.22-3.25, 3.62-3.63, 19.11, 20.1, 20.30-20.32

Arms Export Control Act: §21.52

Artists' Rights and Theft Protection Act of 2005 (the ART Act): §1.8C

Audio Home Recording Act of 1992 (AHRA): §§8.24, 8.27

Child Online Protection Act of 1998 (COPA): §20.20

Child Pornography Prevention Act of 1996 (CPPA): §§20.13, 20.19

Children's Internet Protection Act (CIPA): §20.21

Children's Online Privacy Protection Act of 1998 (COPPA): §§9.28-9.34, 9.36, 9.40, 20.20

Children's Online Privacy Protection Rule: §§9.29, 9.32-9.33

Communications Act of 1934

§230(e)(2): §20.16

Communications Decency Act of 1996 (CDA): §§20.1, 20.4-20.7, 20.18, 20.28

Computer Fraud and Abuse Act (CFAA): §§9.14, 17.28, 18.3-18.7A, 18.9-18.10, 18.12, 18.19, 20.1, 20.38

Computer Maintenance Competition Assurance Act: §1.24

Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act): §§9.6C, 17.11-17.16, 17.18A, 17.19-17.23A, 17.23B, 17.24-17.27, 18.4, 18.7A, 20.1

§5(a)(5): §17.14

Copyright Act: §§1.1, 1.6-1.7, 1.9, 1.12-1.13, 1.16B, 1.17, 1.19, 1.24-1.25A, 1.26-1.27, 1.41, 4.18, 6.9, 7.2, 8.16, 8.23, 8.27, 14.6, 16.27, 20.9, 20.11

§8(b)(1): §17.26

§107: §14.6

§§107-122: §1.18

§201: §1.5

§201(a): §4.18

§512: §1.29

Copyright Revision Act of 1976: §§1.1, 1.7, 20.1

Data Protection Directive: §21.11

Declaratory Judgment Act: §21.4

Digital Millennium Copyright Act of 1998 (DMCA): §§1.1, 1.24-1.25A, 1.26, 1.28, 1.30, 1.34-1.35, 1.37, 1.39, 1.41-1.43, 2.2, 8.2, 8.25, 18.13, 19.1, 21.9

Title I: §§1.25, 20.1

Title II: §1.29

§1201(b): §1.28

Digital Performance Right in Sound Recordings Act of 1995 (DPRA): §§8.25, 8.27

Dot-Kids Implementation and Efficiency Act of 2002 (Dot-Kids Act): §9.35

Economic Espionage Act of 1996: §2.38

Electronic Communications Privacy Act of 1986 (ECPA): §§9.15, 18.6, 18.7A, 18.8-18.11A, 20.1, 21.3

Title I: §§9.15, 18.8-18.10, 18.11A

Title II: §§9.15, 18.8-18.9, 18.11, 20A.5

Electronic Signatures in Global and National Commerce Act (E-Sign): §§7.1, 7.5-7.10, 7.14, 9.24, 10.2

Export Administration Act: §§12.7, 14.16, 21.25

Export Administration Regulations (EAR): §§21.37, 21.39, 21.48, 21.50-21.51, 21.53

Fair Credit Reporting Act: §9.9A

Fair and Accurate Credit Transactions (FACT) Act of 2003: §9.9A

Family Entertainment and Copyright Act: §8.26B

Federal Acquisition Regulations: §14.5

Federal Computer Fraud and Abuse Act: §20.38

Federal Trade Commission Act (FTC Act): §§9.8, 9.9A, 17.2-17.4, 17.6, 17.11, 17.22, 17.29, 20.1

§5: §17.7A

Federal Trademark Dilution Act of 1995 (FTDA): §§3.22, 3.65, 20.29

Foreign Corrupt Trade Practices Act: §12.7

Gramm-Leach-Bliley Financial Modernization Act of 1999: §§9.8, 9.12, 9.22, 20A.2, 22.13

Title V: §9.12

Health Insurance Portability and Accountability Act of 1996 (HIPAA): §§9.8, 9.10-9.11, 20A.2, 22.13

International Emergency Economic Powers Act (IEEPA): §21.25

International Emergency Economic Powers Enhancement Act: §21.25

Internet Tax Freedom Act (ITFA): §§10.17-10.18, 10.20-10.21

Internet Tax Freedom Act Amendments Act of 2007: §10.20

Internet Tax Nondiscrimination Act: §10.21

Lanham Act: §§3.26-3.29, 3.32, 3.35, 3.51-3.52, 3.57, 3.60-3.62, 3.64, 3.71-3.75, 3.77, 3.84-3.85, 16.29-16.30, 17.2-17.3, 17.34, 18.19, 20.1, 20.29

§43(a): §3.84

§43(a)(3): §3.77

Madrid Protocol Implementation Act: §3.48

No Electronic Theft Law (NET Act): §8.26

Omnibus Appropriations Act of 1998: §§10.17, 10.20

Omnibus Crime Control and Safe Streets Act of 1968

Title III: §§9.15, 18.8

Online Copyright Infringement Liability Limitation Act: §1.24

Packers and Stockyards Act: §17.4

Patent Act: §§2.2-2.3, 2.10, 2.15, 16.28-16.29

§261: §16.28

Pen Register Act: §18.11A

Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO-IP Act): §1.17

Prosecutorial Remedies and Tools Against the Exploitation of Children Today Act of 2003

§521: §3.2

Providing Resources, Officers, and Technology to Eradicate Cyber Threats to Our Children Act of 2008 (PROTECT Our Children Act of 2008): §20.13

Racketeer Influenced and Corrupt Organizations Act (RICO): §20.12

Right to Financial Privacy Act of 1978 (RFPA): §9.13

Safe Harbor Accord: §§9.38, 9.40

Sarbanes-Oxley Act of 2002: §20A.2

Securities Act of 1933: §16.35

Sonny Bono Copyright Term Extension Act (CTEA): §1.3

Stored Communications Act (SCA): §§9.15, 18.8, 18.11

Telecommunications Act of 1996

Title V: §20.5

Trademark Act of 1946: §§3.26, 17.3, 20.1

Trademark Dilution Act: §19.11

Trademark Dilution Revision Act of 2006 (TDRA): §3.65-3.66, 3.68

Truth in Domain Names Act: §3.2

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act)

§213: §18.12

§814: §18.12

Uruguay Round Agreements Act

§514: §1.3

Vessel Hull Design Protection Act: §1.24

Wiretap Act: §§9.15, 18.7A, 18.8, 18.11A

SESSION LAWS

Pub L 110-403, §3, 122 Stat 4257: §1.17

Pub L 110-401, 122 Stat 4229: §20.13

Pub L 110-108, 121 Stat 1024: §10.20

Pub L 110-96, 121 Stat 1011: §21.25

Pub L 109-312, 120 Stat 1730: §3.65

Pub L 109-9, 119 Stat 218: §§1.8C, 8.26B

Pub L 108-187, 117 Stat 2699: §§17.12, 18.4, 20.1

Pub L 108-159, 117 Stat 1952: §9.9A

Pub L 108-21, 117 Stat 650: §3.2

Pub L 107-317, 116 Stat 2766: §9.35

Pub L 107-204, 116 Stat 745: §20A.2

Pub L 107-56, 115 Stat 272: §18.12

Pub L 106-554, 113 Stat 2763: §20.21

Pub L 106-113, 113 Stat 1501A: §§19.11, 20.31

Pub L 106-102, 113 Stat 1338: §§9.12, 20A.2

Pub L 106-102, 113 Stat 1332: §9.8

Pub L 105-304, 112 Stat 2860: §§1.1, 1.24, 8.25, 18.13, 19.1

Pub L 105-298, 112 Stat 2827: §1.3

Pub L 105-277, §1203, 112 Stat 2681: §10.18

Pub L 105-277, 112 Stat 2681: §§10.17, 10.20

Pub L 105-147, 111 Stat 2678: §8.26

Pub L 104-191, 110 Stat 1936: §20A.2

Pub L 104-191, 100 Stat 1936: §§9.8, 9.10

Pub L 104-104, 110 Stat 56: §20.5

Pub L 104-98, 109 Stat 985: §19.11

Pub L 104-39, 109 Stat 336: §8.25

Pub L 103-465, 108 Stat 4809: §1.3

Pub L 102-563, 106 Stat 4237: §8.24

Pub L 99-508: §18.10

Pub L 99-508, 100 Stat 1848: §§9.15, 18.8

Pub L 90-351, 82 Stat 211: §§9.15, 18.8

PROPOSED LEGISLATION

HR 1923, 82d Cong, 2d Sess (1952): §2.3

CONGRESSIONAL REPORTS

Senate Reports

105-190: §1.29

104-357: §§18.3, 18.7

100-505: §12.12

95-989: §12.12

House of Representatives Reports

107-240: §10.21

105-796: §1.24

95-595: §12.12

Regulations

CODE OF FEDERAL REGULATIONS

Title 13

120.2: §16.15

120.100-120.102: §16.15

120.150-120.160: §16.15

Title 15

6.4(a)(6)-(7): §21.25

30.2(b): §21.54

30.2(d)(3): §21.54

30.15: §21.54

30.37(f): §21.54

730-774: §§21.21, 21.37, 21.39, 21.48, 21.50-21.51, 21.53

730.3: §21.21

Pt 732: §21.50

732.3(d)(5): §§21.27, 21.37

732.3(h)(1): §21.37

734.2(b)(1): §21.24

734.2(b)(2)(i): §21.24

734.2(b)(2)(ii): §21.24

734.2(b)(3): §21.24

734.2(b)(4)-(5): §21.51

734.2(b)(6): §21.51

734.2(b)(9)(i)(A): §21.24

734.2(b)(9)(iii)(A): §21.58

734.2(b)(9)(iii)(C): §21.58

734.3(a)(1): §21.23

734.3(a)(2): §21.23

734.3(a)(3): §21.23

734.3(b)(3): §§21.23, 21.29, 21.47

734.3(c): §§21.23, 21.27

736.1(c): §21.50

736.2: §21.50

736.2(b)(5): §21.53

Pt 738: §21.28

738.2(a): §21.27

738.2(d): §21.27

Pt 740: §21.41

740.6(a): §21.48

740.7: §21.31

740.7(b)(2): §21.31

740.7(d)(2): §21.31

740.9(c)(2): §21.45

740.9(c)(4)(i): §21.45

740.9(c)(4)(ii)-(iii): §21.45

740.9(c)(5): §21.45

740.9(c)(7): §21.45

740.9(c)(8): §21.45

740.13(a): §21.48

740.13(b): §21.48

740.13(d)(2): §21.48

740.13(e)(1): §21.47

740.13(e)(3): §21.47

740.13(e)(4): §21.46

740.17: §21.40

740.17(a)(1): §21.41

740.17(a)(2): §21.38

740.17(b): §§21.35, 21.48, 21.59

740.17(b)(1): §21.38

740.17(b)(1)(i): §21.41

740.17(b)(2)(iii): §§21.42, 21.46

740.17(b)(2)(iv): §21.44

740.17(b)(3): §21.42

740.17(b)(3)(i): §21.42

740.17(b)(4)(i): §21.34B

740.17(e)(1): §21.59

740.17(e)(1)(iii): §21.59

740.17(e)(2): §21.35

Pt 742: §§21.32, 21.35

742.15: §21.35

742.15(a)(1): §21.41

742.15(b): §§21.33, 21.35, 21.41, 21.46

742.15(b)(1): §21.35

742.15(b)(1)(ii)(B): §21.46

742.15(b)(3): §21.48

742.15(b)(3)(i): §§21.34B, 21.38

742.15(b)(3)(iii): §21.34

742.15(b)(5): §21.33

Pt 744: §§21.33-21.34, 21.52

744.1: §21.53

744.2(a): §21.53

744.3(a): §21.53

744.4(a): §21.53

746.1(a)(1): §21.40

Pt 748: §21.35

748.1(c): §21.35

748.1(d): §21.35

748.3(a): §21.35

748.3(b): §21.35

748.4: §21.35

750.4(a)(2): §21.41

758.1(b)(3): §21.54

758.1(f): §21.54

758.6: §21.55

762.2(a): §21.60

764.3(a)(1)(i): §21.25

764.3(a)(2): §21.25

764.3(b)(2)(i): §21.25

772.1: §§21.30, 21.34A, 21.39, 21.44, 21.48, 21.50

Pt 774: §§21.21, 21.30

Title 16

1.98: §17.7A

2.32: §17.6

255.0: §17.7A

255.0-255.5: §17.7A

255.0(b): §17.7A

255.1(a): §17.7A

255.1(c): §17.7A

255.1, Example 5: §17.7A

255.2: §17.7A

255.5: §17.7A

255.5, Example 7: §17.7A

310.7: §17.6

312.1-312.12: §§9.29-9.32

312.4(b): §9.29

312.5: §9.32

312.5(b): §9.32

312.5(b)(2): §9.32

314.1(a): §9.12

314.2(d): §9.12

314.4: §9.12

314.4(d)(1)-(2): §9.12

316.1-316.6: §§17.12, 17.18A

316.2(m): §17.18A

316.2(p): §17.17

316.3: §17.13

316.3(a)(1): §17.13

316.3(a)(2)(i): §17.13

316.3(a)(2)(ii): §17.13

316.3(a)(3)(i): §17.13

316.3(c): §17.13

316.4(a)(1): §17.20

316.4(a)(2): §17.20

316.5: §17.16

435.1: §10.16

435.1(a)(1): §10.16

435.1(b): §10.16

681.2(b)(5): §9.9A

681.2(b)(9): §9.9A

681.2(d): §9.9A

Title 17

240.17a-4: §20A.2

Title 18

316.2(h): §17.14

316.2(m): §17.14

Title 22

120.27: §21.52

127.7: §21.52

Title 31

Ch V, App A: §21.52

pts 500-597: §21.40

Title 37

1.1-1.997: §2.10

1.104: §2.10

2.6: §3.41

2.32(a)(6): §3.41

2.37: §3.44

2.52(b)(3): §3.43

2.71(a): §3.41

2.72: §3.43

2.87: §3.35

2.89(e)(1): §3.35

2.142(b): §3.50

2.142(e): §3.50

2.145: §3.50

2.151: §3.49

3.1-3.41: §§2.15, 3.57

3.16: §3.57

201: §1.34

201.20: §1.7

Title 45

Pt 160: §§9.10-9.11, 20A.2

Pt 162: §§9.10, 20A.2

Pt 164: §§9.10, 20A.2

Subpt A: §§9.10-9.11

Subpt E: §§9.10-9.11

160.102: §9.11

160.103: §9.11

164.502(b): §9.11

164.504(e)(1): §9.11

164.504(e)(2): §9.11

Title 47

64.3100: §17.23A

64.3100(a)(1): §17.23A

64.3100(a)(4): §17.23A

64.3100(b)(1): §17.23A

64.3100(b)(2): §17.23A

64.3100(b)(3): §17.23A

64.3100(b)(4)-(5): §17.23A

64.3100(c)(2): §17.23A

64.3100(c)(8): §17.23A

64.3100(e): §17.23A

Title 48

12.212: §14.5

52.227-14: §14.5

Regulatory Actions

FEDERAL REGISTER

73 Fed Reg 79425 (2008): §1.26

73 Fed Reg 58073 (2008): §1.26

73 Fed Reg 29654 (2008): §17.18A

71 Fed Reg 68472 (2006): §1.26

69 Fed Reg 40345 (2004): §10.20

Court Rules

FEDERAL RULES OF CIVIL PROCEDURE

4(e): §19.4

4(f): §19.2

4(k)(2): §19.4

16: §20A.6

16(b): §20A.7

26: §§20A.6, 20A.16

2006 Amendment Advisory Committee Notes: §§20A.11, 20A.49

26(a)(1)(A)(ii): §20A.8

26(b)(1): §20A.29

26(b)(2)(B): §§20A.11, 20A.18A

26(b)(2)(B) (: §20A.3

26(b)(2)(C): §20A.11

26(b)(5): §20A.9

26(b)(5)(B): §§20A.44-20A.44A

26(c): §2.37

26(f), 2006 Amendment Advisory Committee Notes: §20A.11

26(f)(3): §20A.7

26(f)(3)(C): §§20A.10, 20A.39

26(f)(3)(D): §20A.10

30(b)(6): §20A.30

33: §§20A.6, 20A.30

33(d): §20A.12

34: §§20A.6, 20A.13, 20A.16, 20A.38

2006 Amendment Advisory Committee Notes: §§20A.13-20A.14

34(a): §§20A.9, 20A.13, 20A.16, 20A.30, 20A.38

34(a)(1)(A): §20A.13

34(b): §§20A.40-20A.41

34(b)(1)(C): §§20A.14, 20A.27

34(b)(2)(E): §§20A.39-20A.40, 20A.42

34(b)(2)(E)(i): §20A.43

34(b)(2)(E)(ii): §20A.14

37: §20A.6

2006 Amendment Advisory Committee Notes: §20A.15

37(b)(2)(A)(vi): §20A.28

37(e): §§20A.4, 20A.15

45: §20A.16

45(a)(1)(C): §20A.16

45(d)(1)(B): §20A.16

45(d)(1)(D): §20A.16

45, Form 35: §20A.6

502: §20A.44A

502(b): §20A.44A

FEDERAL RULES OF EVIDENCE

502: §§20A.9, 20A.13, 20A.44A

502(b): §20A.44A

502(b)(1): §20A.44A

502(b)(2): §20A.44A

502(b)(3): §20A.44A

502(c): §20A.44A

Rules and Rulings

INTERNAL REVENUE PUBLICATIONS

15-A (Employer's Supplemental Tax Guide): §4.13

ETHICS

AMERICAN BAR ASSOCIATION

Model Rules Of Professional Conduct

4.3: §§4.2, 5.5

7.1: §17.10C

7.2(c): §17.10C

7.3(a): §17.10C

7.3(c): §17.10C

Formal Opinions

06-442 (Aug. 2006): §20A.36

DISTRICT OF COLUMBIA LEGAL ETHICS COMMITTEE OPINIONS

341 (Sept. 2007): §20A.36

FLORIDA BAR PROFESSIONAL ETHICS OPINIONS

06-2 (Sept. 2006): §20A.36

NEW YORK COMMISSION ON PROFESSIONAL ETHICS OPINIONS

749 (Dec. 14, 2001): §20A.36

UNIFORM CODES AND ACTS

UNIFORM COMMERCIAL CODE

Art 2: §§7.3, 7.12

1-201(37): §7.6

2-204(1): §§7.2-7.3

2-207: §7.2

2-207(2)(b) (former): §7.14

2-606(1)(b): §7.2

Uniform Computer Information Transactions Act (UCITA): §§7.1, 7.4, 7.11, 7.12, 13.3

Uniform Single Publication Act: §20.2

Uniform Trade Secrets Act (UTSA): §2.20

NONGOVERNMENTALORGANIZATION RULES

INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS (ICANN)

Uniform Domain Name Dispute Resolution Policy (URDP): §§3.11-3.12, 3.17, 3.19, 3.24-3.25, 20.1, 20.26, 20.30

UDRP Rules

¶2(b): §3.18, 3.20

¶2(b): §§3.18, 3.20

¶3: §§3.15-3.16, 3.18

¶3(a): §3.18

¶3(b): §3.18

¶3(b)(ii)-(iii): §3.18

¶3(b)(iv): §3.18

¶3(b)(ix)(1): §3.18

¶3(b)(ix)(2): §3.18

¶3(b)(ix)(3): §3.18

¶3(b)(v): §3.18

¶3(b)(vi)-(vii): §3.18

¶3(b)(viii): §3.18

¶3(b)(ix)(1): §3.18

¶3(b)(x): §3.18

¶3(b)(xi): §3.18

¶3(b)(xii): §3.18

¶3(b)(xiii): §3.18

¶3(b)(xiv): §3.18

¶3(b)(xv): §3.18

¶4(a): §§3.13, 3.18, 3.20, 20.30

¶4(a)(i): §§3.18, 3.20

¶4(a)(ii): §3.20

¶4(a)(iii): §3.18, 3.20

¶4(b): §§3.13, 3.18, 3.20

¶4(c): §§3.13, 3.18, 3.20

¶4(i): §3.18

¶4(k): §3.21

¶5: §§3.15, 3.20

¶5(b): §3.20

¶5(b)(i): §3.20

¶5(b)(ii)-(iii): §3.20

¶5(b)(iv)-(v): §3.20

¶5(b)(vi): §3.20

¶5(b)(vii): §3.20

¶5(b)(viii): §3.20

¶5(c): §3.20

¶6: §§3.18, 3.20

¶15: §3.15

¶15(e): §3.20

¶16: §3.15

¶18: §3.25

¶19: §3.18

UDRP Supplemental Rules

¶3: §3.20

¶¶3-4: §3.18

¶7: §§3.18, 3.20

¶10(a): §3.18

¶10(b): §3.20

¶12: §3.20

Annex D: §§3.18, 3.20

Out-of-State Statutes

ARKANSAS CODE ANNOTATED

4-88-603: §17.24

ARIZONA REVISED STATUTES

44-1372: §17.24

ILLINOIS STATUTES

815 ILCS 511/10: §17.24

MAINE REVISED STATUTES ANNOTATED

Title 10, §1497: §17.24

MARYLAND COMMERCIAL LAW CODE ANNOTATED

14-3002: §17.24

22-101—22-816: §7.11

MASSACHUSETTS

Code of Regulations

Title 201, §17.04: §9.27A

Title 201, §17.05: §9.27A

General Laws Annotated

Ch 93H: §9.27A

Ch 231 §59H: §20.25

MISSOURI REVISED STATUTES

407.1123: §17.24

NEVADA REVISED STATUTES

41.730: §17.24

597.970: §9.27A

NEW MEXICO STATUTES

57-12-23: §17.24

NEW YORK CONSOLIDATED LAWS

Civ R §70-a: §20.25

Civ R §76-a: §20.25

CPLR R 3211(g): §20.25

CPLR R 3212(h): §20.25

OKLAHOMA STATUTES

15 Okla St 776.1: §17.24

PENNSYLVANIA STATUTES

18 Pa CS 7661: §17.24

RHODE ISLAND GENERAL LAWS

11-52-4.1: §17.24

TENNESSEE CODE

Tenn Code 47-18-2501: §17.24

VIRGINIA CODE ANNOTATED

§59.1-501.1—59.1-509.2: §7.11

WEST VIRGINIA CODE ANNOTATED

46A-6G-1—46A-6G-5: §17.24

International Treaties and Terms of Trade

Hague Convention on Exclusive Choice of Court Agreements: §21.2

Art 3(c): §21.2

Art 5: §21.2

Art 6: §21.2

North American Free Trade Agreement (NAFTA): §3.32

Paris Convention for the Protection of Industrial Property of March 20, 1883

Art 4: §§2.14, 3.48

Patent Cooperation Treaty (PCT): §2.14

Protocol Relating to the Madrid Agreement Concerning the International Registration of Marks (June 27, 1989) (Madrid Protocol): §3.48

Art 2: §3.48

Art 3: §3.48

Art 4: §3.48

Art 5: §3.48

United Nations Commission on International Trade Law (UNCITRAL): §21.8

WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998: §1.24

Title I: §1.24

Title IV: §1.24

WTO Doc. No. 1-5859, Ministerial Declaration, Ministerial Conf.—Fourth Sess., Doha (Nov. 14, 2001): §10.18

EUROPEAN UNION

Directives

2006/24/EC (Data Retention77 Directive): §§9.37, 21.18A

2002/58/EC: §21.11

2002/38/EC (Value Added Taxes (VAT) Directive): §21.16

2001/29/EC (Copyright Directive): §21.6

2000/31/EC (Electronic Commerce (EC) Directive): §§7.13, 21.15

1999/93/EC (Electronic Signatures (ES) Directive): §7.13

97/7/EC (Directive on Protection of Consumers in Respect to Distance Contracts): §21.14

95/46/EC (Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Privacy Directive)): §§9.1, 9.37-9.38, 9.40, 21.11-21.13, 21.18

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/Table of Cases

Table of Cases

A

A&M Records, Inc. v Heilman (1977) 75 CA3d 554, 142 CR 390, cert denied (1977) 436 US 952: §20.11

A&M Records, Inc. v Napster, Inc. (9th Cir 2001) 239 F3d 1004: §§1.12-1.13, 1.15-1.16, 1.19-1.20, 1.31, 8.27

A.V. v iParadigms (ED Va 2008) 544 F Supp 2d 473, aff'd in part and rev'd in part on other grounds (4th Cir 2009) 562 F3d 630: §7.3

ACLU v Gonzales (ED Pa 2007) 478 F Supp 2d 775, aff'd sub nom ACLU v Mukasey (3d Cir 2008) 534 F3d 181, cert denied (2009) ___ US ___, 173 L Ed 2d 293, 129 S Ct 1032: §20.20

ALS Scan, Inc. v Digital Serv. Consultants (4th Cir 2002) 293 F3d 707, cert denied (2003) 537 US 1105: §19.10

ALS Scan, Inc. v RemarQ Communities, Inc. (4th Cir 2001) 239 F3d 619: §§1.24, 1.37, 1.42

AMF Inc. v Sleekcraft Boats (9th Cir 1979) 599 F2d 341: §§3.60, 3.72, 3.74

AOL, Inc. Version 5.0 Software Litig., In re (SD Fla 2001) 168 F Supp 2d 1359: §§18.3, 18.6

ASCAP, U.S. v (SD NY 2007) 485 F Supp 2d 438: §1.6C

AT&T Corp. v Excel Communications, Inc. (Fed Cir 1999) 172 F3d 1352, cert denied (1999) 528 US 946: §§2.3, 2.19

Academy of Motion Picture Arts & Sciences v Benson (1940) 15 C2d 685, 104 P2d 650: §3.27

Addy v Bliss & Glennon (1996) 44 CA4th 205, 51 CR2d 642: §4.5

Adobe Sys., Inc. v Stargate Software, Inc. (ND Cal 2002) 216 F Supp 2d 1051: §1.23

Advante Int'l Corp v Mintel Learning Technol. (ND Cal, Nov. 21, 2006, No. C 05-01022 JW) 2006 US Dist Lexis 86334: §20A.38

Advertising.com, Inc., In re (Sept. 12, 2005) No. 042-3196: §9.9B

Aerocon Eng'g, Inc. v Silicon Valley Bank (In re World Auxiliary Power Co.) (9th Cir 2002) 303 F3d 1120: §16.27

Aetna Cas. & Sur. Co. v Superior Court (1993) 19 CA4th 320, 23 CR2d 442: §20.39

Agawam Co. v Jordan (1869) 74 US 583, 19 L Ed 177: §2.14

Aimster Copyright Litig., In re (7th Cir 2003) 334 F3d 643, cert denied (2004) 540 US 1107: §8.27

Aimster Copyright Litig., In re (ND Ill 2002) 252 F Supp 2d 634, aff'd (7th Cir 2003) 334 F3d 643, cert denied (2004) 540 US 1107: §1.32

Aitken v Communications Workers of Am. (WD Va 2007) 496 F Supp 2d 653: §17.13

Alappat, In re (Fed Cir 1994) 33 F3d 1526: §§2.3, 2.19

Allen v Ghoulish Gallery (SD Cal, Nov. 20, 2007, No. 06CV371 NLS) 2007 US Dist Lexis 86224: §1.2

Alliance to End Repression v Rochford (ND Ill 1976) 75 FRD 428: §20A.21

Allstate Ins. Co. v Hague (1981) 449 US 302, 66 L Ed 2d 521, 101 S Ct 633: §19.15

Amazon.com, Inc. v Barnes & Noble.com, Inc. (Fed Cir 2001) 239 F3d 1343: §§2.18, 3.83

America Online, Inc. v AT&T Corp. (4th Cir 2001) 243 F3d 812, cert dismissed (2001) 534 US 946: §3.28

America Online, Inc. v National Health Care Discount, Inc. (ND Iowa 2001) 174 F Supp 2d 890: §§17.28, 18.4

America Online, Inc. v National Health Care Discount, Inc. (ND Iowa 2000) 121 F Supp 2d 1255: §§18.4-18.5, 20.38

America Online, Inc. v Pasieka (Fla App 2004) 870 So2d 170: §19.12

America Online, Inc. v St. Paul Mercury Ins. Co. (ED Va 2002) 207 F Supp 2d 459, aff'd (4th Cir 2003) 347 F3d 89: §20.36

America Online, Inc. v Superior Court (2001) 90 CA4th 1, 108 CR2d 699: §19.12

American Bar Ass'n v FTC (D DC 2009) 671 F Supp 2d 64: §9.9A

American Eyewear v Peeper's Sunglasses (ND Tex 2000) 106 F Supp 2d 895: §7.3

American Guar. & Liab. Ins. Co. v Ingram Micro, Inc. (D Ariz, Apr. 19, 2000, No. CIV 99-185 TUC ACM) 2000 US Dist Lexis 7299: §20.36

American Guar. & Liab. Ins. Co. v Ingram Micro, Inc. (D Ariz Apr. 19, 2000, No. CIV 99-185 TUC ACM) 2000 US Dist Lexis 7299: §20.38

American Library Ass'n v U.S. (ED Pa 2002) 201 F Supp 2d 401, rev'd (2003) 539 US 194: §20.21

American Library Ass'n, U.S. v (2003) 539 US 194, 156 L Ed 2d 221, 123 S Ct 2297: §§20.21, 20.23

Amgen v Chugai Pharm. Co. (Fed Cir 1991) 927 F2d 1200: §2.11

Ampex Corp. v Cargle (2005) 128 CA4th 1569, 27 CR3d 863: §20.2

Andersen, Arthur, LLP v U.S. (2005) 544 US 696, 161 L Ed 2d 1008, 125 S Ct 2129: §20A.4

Anthony v Yahoo! Inc. (ND Cal 2006) 421 F Supp 2d 1257: §20.6B

Apple Computer, Inc. v Microsoft Corp. (9th Cir 1994) 35 F3d 1435, cert denied (1995) 513 US 1184: §1.12

Application Group, Inc. v Hunter Group, Inc. (1998) 61 CA4th 881, 72 CR2d 73: §19.20

Aral v EarthLink, Inc. (2005) 134 CA4th 544, 36 CR 3d 229: §7.14

Argueta v Banco Mexicano (9th Cir 1996) 87 F3d 320: §19.12

Arista Records, Inc. v MP3Board, Inc. (SD NY, Aug. 29, 2002) 2002 US Dist Lexis 16165: §1.15

Arthur Andersen LLP v U.S. (2005) 544 US 696, 161 L Ed 2d 1008, 125 S Ct 2129: §20A.4

Asahi Metal Indus. Co. v Superior Court (1987) 480 US 102, 94 L Ed 2d 92, 107 S Ct 1026: §19.7

Ashcroft v ACLU (2004) 542 US 656, 159 L Ed 2d 690, 124 S Ct 2783: §20.20

Ashcroft v Free Speech Coalition (2002) 535 US 234, 152 L Ed 2d 403, 122 S Ct 1389: §§20.13, 20.15, 20.17, 20.19

Ashton-Tate Corp. v Ross (9th Cir 1990) 916 F2d 516: §1.2

Assessment Technols. of WI, LLC v WIREData, Inc. (7th Cir 2003) 350 F3d 640: §1.2

Atari Computer Entertainment Am., Inc. v Bleem, LLC (9th Cir 2000) 214 F3d 1022: §1.19

Atari Games Corp. v Nintendo of Am., Inc. (Fed Cir 1992) 975 F2d 832: §1.19

Atkinson, Judson, Candies, Inc. v Latini-Hohberger Dhimantec (7th Cir 2008) 529 F3d 371: §20A.44A

Atlantic Recording Corp. v Brennan (D Conn 2008) 534 F Supp 2d 278: §1.6B

Audi AG v D'Amato (6th Cir 2006) 469 F3d 534: §3.23

Autotech Technols. LP v AutomationDirect.com, Inc. (ND Ill 2008) 248 FRD 556: §20A.43

Avalon Software, Inc., In re (Bankr D Ariz 1997) 209 BR 517: §16.27

Avery Dennison Corp. v Allendale Mut. Ins. Co. (9th Cir 2002) 310 F3d 1114: §20.36

B

BMG Music v Gonzalez (7th Cir 2005) 430 F3d 888, cert denied (2006) 547 US 1130: §8.28

Baker v Los Angeles Herald Exam'r (1986) 42 C3d 254, 228 CR 206: §20.3

Bally Total Fitness Holding Corp. v Faber (CD Cal 1998) 29 F Supp 2d 1161: §§20.26, 20.29

Bancroft & Masters, Inc. v Augusta Nat'l, Inc. (9th Cir 2000) 223 F3d 1082: §§19.8, 20.11

Bangoura v Washington Post Co. (Ontario Ct App, Sept. 16, 2005, C41379): §21.4

Barcamerica Int'l v Tyfield Importers, Inc. (9th Cir 2002) 289 F3d 589: §3.53

Barcelona.com v Excelentisimo Ayuntamiento de Barcelona (4th Cir 2003) 330 F3d 617: §§3.25, 21.3

Barrett v Rosenthal (2006) 40 C4th 33, 51 CR3d 55: §§20.5-20.7, 20.25

Batzel v Smith (9th Cir 2003) 333 F3d 1018, cert denied (2004) 541 US 1085: §§20.3, 20.5, 20.6A, 20.25

Bayer Corp. v Roche Molecular Sys., Inc. (ND Cal 1999) 72 F Supp 2d 1111: §2.26

Bed & Breakfast Registry, In re (Fed Cir 1986) 791 F2d 157: §3.28

Bensusan Restaurant Corp. v King (2d Cir 1997) 126 F3d 25: §19.3

Berkic v Crichton (9th Cir 1985) 761 F2d 1289, cert denied (1985) 474 US 826: §1.12

Bernhard v Harrah's Club (1976) 16 C3d 313, 128 CR 215, cert denied (1976) 429 US 859: §19.17

Best W. Int'l, Inc. v Doe (D Ariz, July 25, 2006, No. CV061537) 2006 US Dist Lexis 56014: §20.24

Best W. Int'l, Inc. v Furber (D Ariz, Sept. 5, 2008, No. CV-06-1537-PHX-DGC) 2008 US Dist Lexis 70552: §20.6A

Big Island Candies, Inc. v Cookie Corner (D Haw 2003) 269 F Supp 2d 1236: §3.85

Big Island Candies, Inc. v Cookie Corner (D Haw 2003) 244 F Supp 2d 1086: §3.82

Bilski, In re (Fed Cir 2008) 545 F3d 943, cert granted sub nom Bilski v Doll (2009) ___ US ___, 174 L Ed 2d 246, 129 S Ct 2735: §§2.18-2.19

Bird v Parsons (6th Cir 2002) 289 F3d 865: §3.67

Blumenthal v Drudge (D DC 1998) 992 F Supp 44: §19.10

Bonneville Int'l Corp. v Peters (3d Cir 2003) 347 F3d 485: §8.27

Bonneville Int'l Corp. v Peters (ED Pa 2001) 153 F Supp 2d 763, aff'd (3d Cir 2003) 347 F3d 485: §8.25

Bonzi Software, Inc., U.S. v (Feb 18, 2004, Civ Action No. CV-04-1048 RJK): §9.33

Borders Online, LLC v State Bd. of Equalization (2005) 129 CA4th 1179, 29 CR3d 176: §10.24

Boschetto v Hansing (9th Cir 2008) 539 F3d 1011: §§19.1-19.2, 19.6, 19.9-19.10

Bosley Med. Inst. v Kremer (9th Cir 2005) 403 F3d 672: §3.64

Boston Beer Co. LP, In re (Fed Cir 1999) 198 F3d 1370: §3.28

Boston Duck Tours, LP v Super Duck Tours, LLC (D Mass 2007) 527 F Supp 2d 205, rev'd on other grounds (1st Cir 2008)

531 F3d 1: §3.73

Brazil v Dell Inc. (ND Cal, Aug. 3, 2007, No. C-07-01700 RMW) 2007 US Dist Lexis 59095: §7.14

Brenner v Manson (1966) 383 US 519, 16 L Ed 2d 69, 86 S Ct 1033: §2.7

Bridgeport Music, Inc. v Dimension Films, Inc. (6th Cir 2004) 383 F3d 390: §14.17

Broccoli v Echostar Communications Corp. (D Md 2005) 229 FRD 506: §20A.21

Brookdale Univ. Hosp. & Med. Ctr., Inc. v Health Ins. Plan of Greater N.Y. (ED NY, Feb. 13, 2009, No. 07 CV 1471) 2009 US Dist Lexis 11537: §20A.9

Brookfield Communications, Inc. v West Coast Entertainment Corp. (9th Cir 1999) 174 F3d 1036: §§3.72-3.73, 3.76

Brother Records, Inc. v Jardine (9th Cir 2003) 318 F3d 900, cert denied (2003) 540 US 824: §3.68

Brown, People ex rel v PuriTec (2007) 153 CA4th 1524, 64 CR3d 270: §17.9

Brown Bag Software v Symantec Corp. (9th Cir 1992) 960 F2d 1465, cert denied (1992) 506 US 869: §1.12

Bundesverband der Verbraucherzentralen und Verbraucherverbnde-Verbraucherzentrale Bundesverband eV v deutsche internet versicherung AG (Case C-298/07): §21.15

Burger King v Rudzewicz (1985) 471 US 462, 85 L Ed 2d 528, 105 S Ct 2174: §§19.5-19.6

Burnham v Superior Court (1990) 495 US 604, 109 L Ed 2d 631, 110 S Ct 2105: §19.5

C

CDnow, Inc., U.S. v (July 26, 2000) FTC File No. 0023116: §10.16

Cache La Poudre Feeds, LLC v Land O' Lakes, Inc. (D Colo 2007) 244 FRD 614: §20A.21

Cairo, Inc. v CrossMedia Servs., Inc. (ND Cal, Apr. 1, 2005, No. C04-04825) 2005 US Dist Lexis 8450: §7.4

California Compensation Ins. Co. v Industrial Acc. Comm'n (1948) 86 CA2d 861, 195 P2d 880: §4.14

California Innovations, Inc., In re (Fed Cir 2003) 329 F3d 1334: §3.32

Campbell v Acuff-Rose Music, Inc. (1994) 510 US 569, 127 L Ed 2d 500, 114 S Ct 1164: §§1.19, 1.21

Campbell v General Dynamics Gov't Sys. Corp. (D Mass 2004) 321 F Supp 2d 142: §7.14

Capellupo v FMC Corp. (D Minn 1989) 126 FRD 545: §20A.21

Capitol Records, Inc. v Thomas (D Minn 2008) 579 F Supp 2d 1210: §1.6B

Carafano v Metrosplash.com, Inc. (9th Cir 2003) 339 F3d 1119: §§20.5, 20.6A

CardSystems Solutions, Inc., In re (Feb. 23, 2006) FTC File No. 0523148: §9.9A

Carefirst of Maryland, Inc. v Carefirst Pregnancy Ctrs., Inc. (4th Cir 2002) 305 F3d 253: §19.10

Carnival Cruise Lines, Inc. v Shute (1991) 499 US 585, 113 L Ed 2d 622, 111 S Ct 1522: §19.12

Cartoon Network LP, LLLP v CSC Holdings, Inc. (2d Cir 2008) 536 F3d 121, cert denied (2009) ___ US ___, 174 L Ed 2d 595, 129 S Ct 2890: §1.6A

Caspi v Microsoft Network, LLC (NJ Super 1999) 732 A2d 528: §7.3

Cedars-Sinai Med. Ctr. v Superior Court (1998) 18 C4th 1, 74 CR2d 248: §§20A.22, 20A.26

Chamberlain Group, Inc. v Skylink Technols., Inc. (Fed Cir 2004) 381 F3d 1178: §1.25

Chance v Avenue A, Inc. (WD Wash 2001) 165 F Supp 2d 1153: §18.9

Chern v Bank of America (1976) 15 C3d 866, 127 CR 110: §17.9

Chicago Lawyers' Committee for Civil Rights Under Law, Inc. v Craigslist, Inc. (7th Cir 2008) 519 F3d 666: §20.6

Chicago Lock Co. v Fanberg (9th Cir 1982) 676 F2d 400: §§2.24, 2.35

ChoicePoint, Inc., U.S. v (Jan. 26, 2006) FTC File No. 052-3069: §9.9A

Cincom Sys., Inc. v Novelis Corp. (6th Cir 2009) 581 F3d 431: §§1.9, 22.2

Clark Constr. Group v City of Memphis (WD Tenn 2005) 229 FRD 131: §20A.21

Clay v Sun Ins. Office, Ltd. (1964) 377 US 179, 12 L Ed 2d 229, 84 S Ct 1197: §19.15

Clicks Billiards, Inc. v Sixshooters, Inc. (9th Cir 2001) 251 F3d 1252: §§3.27, 3.77, 3.79, 3.87

Cliffdale Assocs., Inc. (1984) 103 FTC 110: §17.4

Clorox Co. v Chemical Bank (TTAB 1996) 40 USPQ2d 1098: §16.29

CoStar Group, Inc. v LoopNet, Inc. (4th Cir 2004) 373 F3d 544: §§1.6A, 1.14

Cohen v California (1971) 403 US 15, 29 L Ed 2d 284, 91 S Ct 1780: §20.15

Coleman (Parent) Holdings, Inc. v Morgan Stanley & Co. (Fla Cir Ct, Mar. 1, 2005, No. 502003CA005045XXOCAL) 2005 WL 679071: §20A.28

Coleman (Parent) Holdings, Inc. v Morgan Stanley & Co. (Fla Cir Ct, Mar. 1, 2005, No. 502003CA005045XXOCAL) 2005 WL 679071, rev'd on other grounds (Fla App 2006) 955 So2d 1124: §20A.2

Columbia Ins. Co. v Seescandy.com (ND Cal 1999) 185 FRD 573: §§20.3, 20.24

Columbia Pictures Television v Krypton Broad. of Birmingham, Inc. (9th Cir 1997) 106 F3d 284, rev'd on other grounds sub nom Feltner v Columbia Pictures Television (1998) 523 US 340: §19.9

Columbia Pictures, Inc. v Bunnell (CD Cal 2007) 245 FRD 443: §20A.29

Comiskey, In re (Fed Cir 2009) 554 F3d 967: §2.18

Community for Creative Non-Violence v Reid (1989) 490 US 730, 104 L Ed 2d 811, 109 S Ct 2166: §§1.5, 4.14

CompuServe, Inc. v Cyber Promotions, Inc. (SD Ohio 1997) 962 F Supp 1015: §§17.28, 18.18

CompuServe, Inc. v Patterson (6th Cir 1996) 89 F3d 1257: §§7.3, 19.9

ComputerXpress, Inc. v Jackson (2001) 93 CA4th 993, 113 CR2d 625: §20.25

Convertino v U.S. Dep't of Justice (D DC, Dec. 10, 2009, No. 04-0236) 2009 US Dist Lexis 115050: §20A.5

Corbis Corp. v Amazon.com, Inc. (WD Wash 2004) 351 F Supp 2d 1090: §20.5

Courtesy Temporary Serv., Inc. v Camacho (1990) 222 CA3d 1278, 272 CR 352: §2.23

Creative Computing v Getloaded.com (9th Cir 2004) 386 F3d 930: §18.5

Cubby, Inc. v CompuServe, Inc. (SD NY 1991) 776 F Supp 135: §20.4

Cyber Promotions, Inc. v America Online, Inc. (ED Pa 1996) 948 F Supp 436: §§17.28, 20.24

Cyberheat, Inc., U.S. v (D Ariz, Mar. 2, 2007, No. CV 05-457-TUC-DCB) 2007 US Dist Lexis 15448: §17.21

Cybersell, Inc. v Cybersell, Inc. (9th Cir 1997) 130 F3d 414: §§19.1, 19.9

D

DSM Pharms., Inc., In re (TTAB 2008) 87 USPQ2d 1623: §3.38

DSW Inc., In re (Dec. 1, 2005) No. 052-3096: §9.9A

Daly v Viacom, Inc. (ND Cal 2002) 238 F Supp 2d 1118: §20.9

Daniel Orifice Fitting Co. v Whalen (1962) 198 CA2d 791, 18 CR 659: §4.9

Danjaq, LLC v Sony Corp. (CD Cal Mar. 11, 1999, CV-978414-ER) 1999 US Dist Lexis 22486: §2.26

Dart v Craigslist. Inc. (ND Ill 2009) 665 F Supp 2d 961: §20.6

Dawn Donut Co. v Hart's Food Stores, Inc. (2d Cir 1959) 267 F2d 358: §3.53

DeGidio v West Group Corp. (6th Cir 2004) 355 F3d 506, cert denied (2004) 542 US 904: §§3.28-3.29

Delfino v Agilent Technols., Inc. (2006) 145 CA4th 790, 52 CR3d 376: §20.5

Delta Computer Corp. v Walter J. Frank, Inc. (5th Cir 1999) 196 F3d 589: §20.39

Deltek, Inc. v Iuvo Sys., Inc. (ED Va, Apr. 20, 2009, No. 1:09cv330) 2009 US Dist Lexis 33555: §3.73

Dendrite Int'l, Inc. v Doe 3 (NJ Super 2001) 775 A2d 756: §20.24

Designer Skin, LLC v S&L Vitamins, Inc. (D Ariz 2008) 560 F Supp 2d 811: §3.73

DiGiorgio Fruit Corp. v AFL-CIO (1963) 215 CA2d 560, 30 CR 350: §20.2

Diamond v Chakrabarty (1980) 447 US 303, 65 L Ed 2d 144, 100 S Ct 2204: §2.3

Diamond v Diehr (1981) 450 US 175, 67 L Ed 2d 155, 101 S Ct 1048: §§2.3, 2.19

Dible v Haight Ashbury Free Clinics, Inc. (2009) 170 CA4th 843, 88 CR3d 464: §20.2

Diepenhorst v City of Battle Creek (WD Mich, June 30, 2006, No. 1:05-cv-734) 2006 US Dist Lexis 48551: §20A.38

Direct Revenue, LLC, People v (Sup Ct 2008) 862 NYS2d 816: §18.17

Disc Golf Ass'n Inc. v Champion Disc, Inc. (9th Cir 1998) 158 F3d 1002: §3.81

Doe v America Online (Fla 2001) 783 So2d 1010: §20.7

Doe v Cahill (Del Super 2005) 884 A2d 451: §20.24

Doe v Friendfinder Network, Inc. (D NH 2008) 540 F Supp 2d 288: §20.6C

Doe v MySpace Inc. (5th Cir 2008) 528 F3d 413: §20.6

Doe v MySpace, Inc. (ED Tex 2009) 629 F Supp 2d 663: §20.6

Doe II v MySpace Inc. (2009) 175 CA4th 561, 96 CR3d 148: §20.6

Donna v Dodd, Mead & Co. (SD NY 1974) 374 F Supp 429: §1.4

DoubleClick Inc. Privacy Litig., In re (SD NY 2001) 154 F Supp 2d 497: §§18.6, 18.9

Douglas v District Court (9th Cir 2007) 495 F3d 1062: §§7.14, 8.3

Dow Jones & Co. v Gutnick [2002] HCA 56 (10 Dec 2002): §§19.18, 21.4

Dow Jones & Co. v Harrods, Ltd. (SD NY 2002) 237 F Supp 2d 394, aff'd (2d Cir 2003) 346 F3d 357: §21.4

Downing v Abercrombie & Fitch (9th Cir 2001) 265 F3d 994: §20.9

Dr. Seuss Enters., L.P. v Penguin Books USA, Inc. (9th Cir 1997) 109 F3d 1394, cert dismissed (1997) 521 US 1146: §3.73

Drew, U.S. v (CD Cal 2009) 259 FRD 449: §18.5

Drew, U.S. v (CD Cal, May 15, 2008, No. CR-08-0582-GW): §18.5

Dubilier Condenser Corp., U.S. v (1933) 289 US 178, 77 L Ed 1114, 53 S Ct 554: §4.7

Dyer v Childress (2007) 147 CA4th 1273, 55 CR3d 544: §20.25

E

e360Insight, LLC v Comcast Corp. (ND Ill 2008) 546 F Supp 2d 605: §20.6D

E*Trade Secs. LLC v Deutsche Bank AG (D Minn 2005) 230 FRD 582: §§20A.21, 20A.28

E. & J. Gallo Winery v Gallo Cattle Co. (9th Cir 1992) 967 F2d 1280: §§3.57, 16.29

EF Cultural Travel BV v Zefer Corp. (1st Cir 2003) 318 F3d 58: §18.5

EarthLink, Inc. v Carmack (ND Ga, May 7, 2003, No. 1:02-CV-3041-TWT) 2003 US Dist Lexis 9963: §17.28

eBay, Inc. v Bidder's Edge, Inc. (ND Cal 2000) 100 F Supp 2d 1058: §§8.17, 18.18, 18.20

eBay, Inc. v MercExchange, LLC (2006) 547 US 388, 164 L Ed 2d 641, 126 S Ct 1837: §2.17A

Echo Travel, Inc. v Travel Assocs., Inc. (1989) 870 F2d 1264: §3.61

Educ. Research Ctr. of Am., Inc., In re (May 9, 2003) No. C-4079: §9.9A

Edwards v Arthur Andersen LLP (2008) 44 C4th 937, 81 CR3d 282: §2.26

Effects Assocs., Inc. v Cohen (9th Cir 1990) 908 F2d 555, cert denied (1991) 498 US 1103: §5.26

Egilman v Keller & Heckman, LLP (D DC 2005) 401 F Supp 2d 105: §1.25

Eilberg, In re (TTAB 1998) 49 USPQ2d 1955: §3.45

ElCom Ltd., U.S. v (ND Cal 2002) 203 F Supp 2d 1111: §1.28

Eldred v Ashcroft (2003) 537 US 186, 154 L Ed 2d 683, 123 S Ct 769: §1.3

Elektra Entertainment Group, Inc. v Barker (SD NY 2008) 551 F Supp 2d 234: §1.6B

Elektra Entertainment Group, Inc. v O'Brien (ND Cal, Mar. 2, 2007, No. CV 06-5289 SJO (MANx): §8.28

Eli Lilly & Co. v Natural Answers Inc. (7th Cir 2000) 233 F3d 456: §3.74

Ellison v Robertson (9th Cir 2004) 357 F3d 1072: §§1.13, 1.31, 1.34, 1.42

Ellison v Robertson (CD Cal 2002) 189 F Supp 2d 1051: §1.31

Environmental Designs, Ltd. v Union Oil Co. (Fed Cir 1983) 713 F2d 693, cert denied (1984) 464 US 1043: §2.9

Envirotech Corp. v Westech Eng'g, Inc. (Fed Cir 1990) 904 F2d 1571: §2.13

Eolas Technols., Inc. v Microsoft Corp. (ND Ill, Jan. 14, 2004, No. 99C0626) 2004 US Dist Lexis 534, aff'd in part and rev'd in part (Fed Cir 2005) 399 F3d 1325: §2.19

Esrim Ve Sheva Holding Corp., In re (Dec. 17, 2001) FTC File No. 012 3116: §17.7

Everex Sys. v Cadtrak Corp. (In re CFLC, Inc.) (9th Cir 1996) 89 F3d 673: §2.15

Ex parte Odol-Werke Wien Gesellschaft M.B.H. (Comm'r Pats 1956) 111 USPQ 286: §3.44

Ex parte Wembley, Inc. (Comm'r Pats 1956) 111 USPQ 386: §3.27

F

FTC v Cleverlink Trading Ltd. (ND Ill 2007) 519 F Supp 2d 784: §7.8

FTC v Gem Merchandising Corp. (11th Cir 1996) 87 F3d 466: §17.6

FTC v Global Net Solutions, Inc. (D Nev 2005) Civ Action No. CV-S-05-0002-PMP-LRL: §17.22

FTC v Myricks d/b/a MP3DownloadCity.com (CD Cal 2006, Civ Action No. CV-05-7013): §17.7

FTC v Odysseus Mktg., Inc. (D NH 2005) Civ Case No. 05-CV-330 SM: §17.22

FTC v Salyon, Inc. (Nov. 6, 2001) FTC File No. 01 23124: §17.7

FTC v Sili Neutraceuticals, LLC (ND Ill 2007) Civil Action No. 07C 4541.: §17.22

FTC v Vital Dynamics, Inc. (Dec. 26, 2002) FTC File No. 012 3249: §17.7

FTC v Zuccarini (ED Pa, Apr. 10, 2002, No. 01-CV-4854) 2002 US Dist Lexis 13324: §17.7

Fabrication Enters. v Hygenic Corp. (2d Cir 1995) 64 F3d 53: §3.77

Facebook, Inc. v ConnectU LLC (ND Cal 2007) 489 F Supp 2d 1087: §17.26

Fair Hous. Council v Roommates.com, LLC (9th Cir 2008) 521 F3d 1157: §20.6B

Falwell & Anor v Cohn & Ors, WIPO Case No. D2002-0184: §20.30

Faulkner v National Geographic Soc'y (SD NY 2002) 211 F Supp 2d 450: §3.61

Feist Publications, Inc. v Rural Tel. Serv. Co. (1991) 499 US 340, 113 L Ed 2d 358, 111 S Ct 1282: §1.2

Fenix Cattle Co. v Silver (In re Select-A-Seat) (9th Cir 1980) 625 F2d 290: §12.12

Field v Google, Inc. (D Nev 2006) 412 F Supp 2d 1106: §§1.19, 1.32

FileNet Corp. v Chubb Corp. (NJ App 1999) 735 A2d 1170: §20.39

FirstEnergy Corp. Sec. Litig., In re (ND Ohio 2004) 229 FRD 541: §20A.25

Fisher v Dees (9th Cir 1986) 794 F2d 432: §14.17

Fletcher v San Jose Mercury News (1989) 216 CA3d 172, 264 CR 699: §20.3

Florida Bar v Went For It, Inc. (1995) 515 US 618, 132 L Ed 2d 541, 115 S Ct 2371: §17.11

Foley v Interactive Data Corp. (1988) 47 C3d 654, 254 CR 211: §4.3

Fonar Corp. v General Elec. Co. (Fed Cir 1997) 107 F3d 1543, cert denied (1997) 522 US 908: §2.11

Fonovisa, Inc. v Cherry Auction, Inc. (9th Cir 1996) 76 F3d 259: §§1.13, 1.16

Fonovisa, Inc. v Napster, Inc. (ND Cal, Jan. 28, 2002) 2002 US Dist Lexis 4270: §§1.13, 1.15

Ford Motor Co. v Lapertosa (ED Mich 2001) 126 F Supp 2d 463: §3.65

Forrest v Verizon Communications, Inc. (DC App 2002) 805 A2d 1007: §7.3

Forrester, U.S. v (9th Cir 2008) 512 F3d 500: §9.7

Franklin v Dynamic Details, Inc. (2004) 116 CA4th 375, 10 CR3d 429: §20.3

Fraser v Nationwide Mut. Ins. Co. (3d Cir 2003) 352 F3d 107: §§9.15, 18.8

Friends of Kathleen Kennedy Townsend v B.G. Birt, WIPO Case No. D2002-0451: §20.30

Fuddruckers, Inc. v Doc's B.R. Others, Inc. (9th Cir 1987) 826 F2d 837: §§3.77, 3.80, 3.87

Fugate v Phoenix Civil Serv. Bd. (9th Cir 1986) 791 F2d 736: §9.7

G

Gates Rubber Co. v Bando Chem. Indus., Ltd. (D Colo 1996) 167 FRD 90: §20A.31

Gateway Learning Corp., In re (July 7, 2004) FTC File No. 042-3047: §§7.14, 9.9

Gateway, Inc., In re (May 15, 2001) FTC File No. 992 3276: §§17.5, 17.7

Gencor Indus., Inc. v Wausau Underwriters Ins. Co. (MD Fla 1994) 857 F Supp 1560: §20.39

Genica Corp., In re (Feb. 5, 2009) FTC File No. 082 3113: §9.9A

Gentry v eBay, Inc. (2002) 99 CA4th 816, 121 CR2d 703: §§20.5, 20.7

GeoCities, a Corp., In re (Feb. 5, 1999) No. C-3850: §9.9

Gershwin Publ. Corp. v Columbia Artist Mgmt., Inc. (2d Cir 1971) 443 F2d 1159: §§1.13, 1.16

Gertz v Robert Welch, Inc. (1974) 418 US 323, 41 L Ed 2d 789, 94 S Ct 2997: §§20.2-20.3

Gibson v Craigslist, Inc. (SD NY, June 15, 2009, No. 08 Civ 7735) 2009 US Dist Lexis 53246: §20.6

Ginsberg v New York (1968) 390 US 629, 20 L Ed 2d 195, 88 S Ct 1274: §20.17

Gionfriddo v Major League Baseball (2001) 94 CA4th 400, 114 CR2d 307: §20.9

Glaverbel Societe Anonyme v Northlake Mktg. & Supply, Inc. (Fed Cir 1995) 45 F3d 1550: §2.8

Global Telemedia Int'l, Inc. v Doe 1 (CD Cal 2001) 132 F Supp 2d 1261: §§20.3, 20.25

Goddard v Google, Inc. (ND Cal 2009) 640 F Supp 2d 1193: §20.6B

Goddard v Google, Inc. (ND Cal, Dec. 17, 2008, No. C 08-2738 JF (PVT) 2008 US Dist Lexis 101890: §20.6

Godfrey v Demon Internet Ltd. (1999) 4 All ER 342 (QBD), (2000) 3 WLR 1020, (2001) QB 201: §21.3

Golan v Gonzales (10th Cir 2007) 501 F3d 1179: §1.3

Goldhaber v Kohlenberg (NJ Super 2007) 928 A2d 948: §19.3

Gooding, Warden v Wilson (1972) 405 US 518, 31 L Ed 2d 408, 92 S Ct 1103: §20.15

Goodman v Praxair Servs., Inc. (D Md 2009) 632 F Supp 2d 494: §§20A.21-20A.22

Google Inc. v American Blind & Wallpaper Factory, Inc. (ND Cal, Apr. 18, 2007, No. C03-5340 JF (RS)) 2007 US Dist Lexis 32450: §3.73

Gorman v Ameritrade Holding Corp. (DC Cir 2002) 293 F3d 506: §19.8

Goss Int'l Ams., Inc. v A-American Mach. & Assembly Co. (ND Ill, Nov. 30, 2007, No. 07C3248) 2007 US Dist Lexis 88382: §1.8A

Government Employees Ins. Co. v Google, Inc. (ED Va 2004) 330 F Supp 2d 700: §3.73

Graham v John Deere Co. (1966) 383 US 1, 15 L Ed 2d 545, 86 S Ct 684: §2.9

Greenly v Cooper (1978) 77 CA3d 382, 143 CR 514: §2.23

Gross, William A., Constr. Assocs., Inc. v American Mfrs. Mut. Ins. Co. (SD NY 2009) 256 FRD 134: §20A.4

Gucci Am., Inc. v Hall & Assocs. (SD NY 2001) 135 F Supp 2d 409: §20.6C

H

Hagenbuch v 3B6 Sistemi Elettronici Industriali SRL (ND IL, Mar. 8, 2006, No. 04 C 3 109) 2006 US Dist Lexis 10838: §§20A.42-20A.43

Hall v LaRonde (1997) 56 CA4th 1342, 66 CR2d 399: §19.9

Hanover Star Milling Co. v Metcalf (1916) 240 US 403, 60 L Ed 713, 36 S Ct 357: §3.31

Harper & Row, Publishers, Inc. v Nation Enters. (1985) 471 US 539, 85 L Ed 2d 588, 105 S Ct 2218: §§1.18, 1.21-1.22

Harris v Blockbuster Inc. (ND Tex 2009) 622 F Supp 2d 396: §7.14

Harrods Ltd. v Dow Jones & Co., Inc. (2003) EWHC 1162 (QB): §21.4

Harrods Ltd. v Sixty Internet Domain Names (4th Cir 2002) 302 F3d 214: §3.22

Healix Infusion Therapy, Inc. v Murphy (SD Tex, Sept. 2, 2008, No. H-08-0337) 2008 US Dist Lexis 67723: §3.23

Healthcare Advocates, Inc. v Harding, Earley, Follmer & Frailey (ED Pa 2007) 497 F Supp 2d 627: §20.11

Helen Folsade aka Sade v Quantum Computer Servs. Inc., WIPO Case No. D2000-0794: §20.30

Hendrickson v Amazon.com, Inc. (CD Cal 2003) 298 F Supp 2d 914: §1.37

Hendrickson v eBay, Inc. (CD Cal 2001) 165 F Supp 2d 1082: §§1.29, 1.35-1.37, 1.42

Heriot v Byrne (ND Ill 2009) 257 FRD 645: §20A.44A

Hernandez v Hillsides (2009) 47 C4th 272, 97 CR3d 274: §9.17

Hershey Foods, U.S. v (Mar. 6, 2003, Civ. Action No. 4:CV03-350): §9.33

Higher Balance, LLC v Quantum Future Group, Inc. (D Ore, Dec. 18, 2008, No. 08-233-HA) 2008 US Dist Lexis 102611: §20.6A

Hill v Gateway 2000, Inc. (7th Cir 1997) 105 F3d 1147: §7.2

Hines v Overstock.com, Inc. (ED NY, Sept. 8, 2009, No. 09 CV 991) 2009 US Dist Lexis 81204: §7.4

Hockings, U.S. v (9th Cir 1997) 129 F3d 1069: §20.13

Holiday Inn v Holiday Inns, Inc. (CCPA 1976) 534 F2d 312: §3.40

Home Indem. Co. v Hyplains Beef (D Kan 1995) 893 F Supp 987, aff'd without opinion (10th Cir 1996) 89 F3d 850: §20.40

Homer TLC, Inc. v GreenPeople (Oct. 25, 2005) Nat'l Arbitration Forum Case No. FA0508000550345: §20.26

Hormel Foods Corp. v Jim Henson Prods., Inc. (2d Cir 1996) 73 F3d 497: §3.65

Horphag Research Ltd. v Pellegrini (9th Cir 2003) 337 F3d 1036, cert denied (2004) 540 US 1111: §§3.68, 3.72

Hotaling v Church of Jesus Christ of Latter-Day Saints (4th Cir 1997) 118 F3d 199: §1.6B

Hotel Sec. Checking Co. v Lorraine Co. (2nd Cir 1908) 160 F 467: §2.18

Hotmail Corp. v Van$ Money Pie, Inc. (ND Cal, Apr. 16, 1998, C98-20064-JW) 1998 US Dist Lexis 10729: §7.3

Hynix Semiconducter, Inc. v Rambus, Inc. (ND Cal 2006) 591 F Supp 2d 1038: §20A.4

Hypertouch, Inc. v Kennedy-W. Univ. (ND Cal, Mar. 8, 2006, No. C04-05203 SI) 2006 US Dist Lexis 14673: §17.22

I

IMX, Inc. v Lending Tree, LLC (D Del 2005) 79 USPQ2d 1373: §2.10

IQ Group v Wiesner Publ'g, LLC (D NJ 2006) 409 F Supp 2d 587: §1.25A

Iconix Brand Group, Inc., U.S. v (Nov. 5, 2009, Civ Action No. 09 Civ 8864 (MGC): §9.33

Iconix, Inc. v Tokuda (ND Cal 2006) 457 F Supp 2d 969: §§1.2, 4.10

In re _____ (*see* name of party)

Integral Systems, Inc. v Peoplesoft, Inc. (ND Cal, July 19, 1991) 1991 US Dist LEXIS 20878: §3.78

Intel Corp. v Hamidi (2003) 30 C4th 1342, 71 P3d 296, 1 CR3d 32: §18.20

Interactive Network, Inc. v NTN Communications (ND Cal 1995) 875 F Supp 1398: §§3.78, 3.83

International Shoe Co. v Washington (1945) 326 US 310, 90 L Ed 95, 66 S Ct 154: §§19.1, 19.5-19.6, 19.8, 19.10

International Transactions, Ltd. v Embotelladora Agral Regiomontana, SA de CV (5th Cir 2003) 347 F3d 589: §21.5

Interstellar Starship Servs., Ltd. v EPIX, Inc. (9th Cir 2002) 304 F3d 936: §§3.23, 3.63, 17.3

Intuit Privacy Litig., In re (CD Cal 2001) 138 F Supp 2d 1272: §18.9

Inwood Labs., Inc. v Ives Labs., Inc. (1982) 456 US 844, 72 L Ed 2d 606, 102 S Ct 2182: §§3.34, 3.60

Io Group, Inc. v Veoh Networks, Inc. (ND Cal 2008) 586 F Supp 2d 1132: §1.35

Iomega Corp., U.S. v (Dec. 9, 1998) Civ Act No. 1:98CV00141C, FTC File No. 972 3023: §10.16

Iowa State Univ. Research Found., Inc. v American Broad. Cos. (2d Cir 1980) 621 F2d 57: §1.18

Israel Harold Asper v Communication X Inc., WIPO Case No. D2001-0540: §20.30

iXL, Inc. v AdOutlet.com, Inc. (ED Ill 2001) 2001 US Dist Lexis 3784: §5.12

J

J.G. Wentworth, S.S.C. LP v Settlement Funding LLC (ED Pa, Jan. 4, 2007, No. 06-0597) 2007 US Dist Lexis 288: §3.73

Jacobsen v Katzer (Fed Cir 2008) 535 F3d 1373: §§8.8, 14.18

Jada Toys, Inc. v Mattel, Inc. (9th Cir 2008) 518 F3d 628: §3.60

Jaynes v Commonwealth (Va 2008) 666 SE2d 303: §20.24

Jensen v Hewlett-Packard Co. (1993) 14 CA4th 958, 18 CR2d 83: §20.2

Jews for Jesus v Brodsky (D NJ 1998) 993 F Supp 282, aff'd without opinion (3d Cir 1998) 159 F3d 1351: §20.29

John B. v Goetz (6th Cir 2008) 531 F3d 448: §20A.22

John Doe Antiterrorism Officer v City of New York (SD NY 2008) 583 F Supp 2d 444: §20.6A

Johnson v Microsoft Corp. (WD Wash, June 23, 2009, No. C06-0900RAJ) 2009 US Dist Lexis 58174: §9.6

Johnson Controls, Inc. v Phoenix Control Sys., Inc. (9th Cir 1989) 886 F2d 1173: §1.2

Joseph v 1200 Valencia, Inc. (In re 199Z, Inc.) (Bankr CD Cal 1992) 137 BR 778: §16.29

Judson Atkinson Candies, Inc. v Latini-Hohberger Dhimantec (7th Cir 2008) 529 F3d 371: §20A.44A

Julia Fiona Roberts v Russell Boyd, WIPO Case No. D2000-210: §20.30

K

KP Permanent Make-Up, Inc. v Lasting Impression, Inc. (2004) 543 US 111, 160 L Ed 2d 440, 125 S Ct 542: §3.64

KSR Int'l Co. v Teleflex Inc. (2007) 550 US 398, 167 L Ed 2d 705, 127 S Ct 1727: §2.9

Kalow & Springnut, LLP v Commence Corp. (D NJ, June 23, 2008, No. 07-3442(FLW)) 2008 US Dist Lexis 48036: §18.6

Kearney v Salomon Smith Barney, Inc. (2006) 39 C4th 95, 45 CR3d 730: §19.17

Keene Corp. v Paraflex Indus., Inc. (3d Cir 1981) 653 F2d 822: §3.82

Keeton v Hustler Magazine, Inc. (1984) 465 US 770, 79 L Ed 2d 790, 104 S Ct 1473: §19.6

Kellogg Co. v National Biscuit Co. (1938) 305 US 111, 83 L Ed 73, 59 S Ct 109: §3.28

Kelly v Arriba Soft Corp. (9th Cir 2003) 336 F3d 811: §§1.19, 1.22, 8.15

Kentucky Fried Chicken Corp. v Diversified Packaging Corp. (5th Cir 1977) 549 F2d 368: §3.53

King v Burstein (2004) EWCA Civ 1329: §21.4

Kohler Co. v Moen Inc. (7th Cir 1993) 12 F3d 632: §3.77

Konop v Hawaiian Airlines, Inc. (9th Cir 2002) 302 F3d 868, cert denied (2003) 537 US 1193: §§18.8, 18.11

Koresko v RealNetworks, Inc. (ED Cal 2003) 291 F Supp 2d 1157: §§7.3, 19.12

Kremen v Cohen (9th Cir 2003) 337 F3d 1024: §§3.9, 20.11

Krinsky v Doe 6 (2008) 159 CA4th 1154, 72 CR3d 231: §20.3

L

LVRC Holdings LLC v Brekka (9th Cir 2009) 581 F3d 1127: §18.7

La Resolana Architects PA v Clay Realtors Angel Fire (10th Cir 2005) 416 F3d 1195: §1.8A

Lahoti v VeriCheck, Inc. (9th Cir 2009) 586 F3d 1190: §§3.23, 3.27-3.28, 3.30

Landmark Communications, Inc., In re (TTAB 1979) 204 USPQ 692: §3.27

Landscape Forms, Inc. v Columbia Cascade Co. (2d Cir 1997) 113 F3d 373: §3.85

Lawrence v Texas (2003) 539 US 558, 156 L Ed 2d 508, 123 S Ct 2472: §9.7

Laws v Sony Music Entertainment, Inc. (9th Cir 2006) 448 F3d 1134: §20.9

Lenz v Universal Music Corp. (ND Cal, Oct. 28, 2008, No. C07-3783JF(RS)) 2008 US Dist Lexis 91890: §1.37

Les Halles de Paris, In re (Fed Cir 2003) 334 F3d 1371: §3.32

Levi Strauss & Co. v Blue Bell, Inc. (9th Cir 1980) 632 F2d 817: §3.29

Lexmark Int'l, Inc., v Static Control Components, Inc. (6th Cir 2004) 387 F3d 522: §1.25

Libman Co. v Vining Indus. (7th Cir 1995) 69 F3d 1360, cert denied (1996) 517 US 1234: §3.87

Lion Mfg. Corp. v Chicago Flexible Shaft Co. (9th Cir 1939) 106 F2d 930: §4.7

Lockheed Martin Corp. v Network Solutions, Inc. (9th Cir 1999) 194 F3d 980: §3.60

Long v Walt Disney Co. (2004) 116 CA4th 868, 10 CR3d 836: §20.2

Los Angeles News Serv. v Tullo (9th Cir 1992) 973 F2d 791: §§1.20-1.22

Lotus Dev. Corp. v Borland Int'l, Inc. (1st Cir 1995) 49 F3d 807, aff'd (1996) 516 US 233: §§1.2, 3.78

Louis Vuitton Malletier, S.A. v Akanoc Solutions, Inc. (ND Cal 2008) 591 F Supp 2d 1098: §3.60

Lowry, In re (Fed Cir 1994) 32 F3d 1579: §2.3

Lubrizol Enters., Inc. v Richmond Metal Finishers, Inc. (4th Cir 1985) 756 F2d 1043, cert denied (1986) 475 US 1057: §12.12

Lucent Techs., Inc. v Lucentsucks.com (ED Va 2000) 95 F Supp 2d 528: §20.31

Lulirama Ltd, Inc. v Axcess Broad. Servs., Inc. (5th Cir 1997) 128 F3d 872: §1.9

M

M/S Bremen v Zapata Off-Shore Co. (1972) 407 US 1, 32 L Ed 2d 513, 92 S Ct 1907: §19.12

MAI Sys. Corp. v Peak Computer, Inc. (9th Cir 1993) 991 F2d 511: §§1.6A, 1.16B

MGM Studios, Inc. v Grokster, Ltd. (CD Cal 2007) 518 F Supp 2d 1197: §8.27

Macys.com, Inc., U.S. v (July 26, 2000) FTC File No. 0023114: §10.16

Magnetic Data Inc. v St. Paul Fire & Marine Ins. Co. (Minn 1989) 442 NW2d 153: §§20.36-20.37

Malletier, Louis Vuitton, S.A. v Akanoc Solutions, Inc. (ND Cal 2008) 591 F Supp 2d 1098: §3.60

Mancia v Mayflower Textile Servs. Co. (D Md 2008) 253 FRD 354: §20A.4

Marino v Video Images Prods., WIPO Case No. D2000-0598: §20.30

Mark Warner 2001 v Mike Larson, Nat'l Arbitration Forum Case Case No. FA0009000095746, Nov. 15: §20.30

Markman v Westview Instruments, Inc. (1996) 517 US 370, 134 L Ed 2d 577, 116 S Ct 1384: §2.11

Markman v Westview Instruments, Inc. (Fed Cir 1995) 52 F3d 967, aff'd (1996) 517 US 370: §2.12

Marlar v Yellow Transp. (WD Mo, Nov. 29, 2004, No. 03-1042-CV-W-HFS) 2004 US Dist Lexis 26653: §7.14

Marobie-Fl, Inc. v National Ass'n of Fire Equip. Distribs. (ND Ill 1997) 983 F Supp 1167: §8.20

Mattel, Inc. v Internet Dimension, Inc. (SD NY, July 13, 2000, No. 99 CIV 10066) 2000 US Dist Lexis 9747: §§3.22, 3.66

Mattel, Inc. v MCA Records Inc. (9th Cir 2002) 296 F3d 894, cert denied (2003) 537 US 1171: §3.65

Mattel, Inc. v Procount Bus. Serv. (SD NY, Mar. 10, 2004, No. 03 Civ 7234 (RWS)) 2004 US Dist Lexis 3895: §19.9

Mazur v eBay Inc. (ND Cal, July 25, 2008, No. C 07-03967 MHP) 2008 US Dist Lexis 57105: §20.12

McClain v Ortmayer (1891) 141 US 419, 35 L Ed 800, 12 S Ct 76: §2.11

McIntyre v Ohio Elections Comm'n (1995) 514 US 334, 131 L Ed 2d 426, 115 S Ct 1511: §20.24

McKinney v County of Santa Clara (1980) 110 CA3d 787, 168 CR 89: §20.2

Mead Data Cent. v Toyota Motor Sales USA, Inc. (2d Cir 1989) 875 F2d 1026: §3.65

MedImmune, Inc. v Genentech (2007) 549 US 118, 166 L Ed 2d 604, 127 S Ct 764: §2.17A

MercExchange, LLC v eBay, Inc. (Fed Cir 2005) 401 F3d 1323: §2.17A

MercExchange, LLC v eBay, Inc. (Fed Cir 2005) 401 F3d 1323, vacated on other grounds (2006) 547 US 946: §2.18

MercExchange, LLC v eBay, Inc. (ED Va 2003) 275 F Supp 2d 695: §2.18

Merck & Co. Inc. v Lyon (MD NC 1996) 941 F Supp 1443: §2.26

Metcalf v Bochco (9th Cir 2002) 294 F3d 1069: §1.12

Metro-Goldwyn-Mayer Studios, Inc. v Grokster, Ltd. (2005) 545 US 913, 162 L Ed 2d 781, 125 S Ct 2764: §§1.16A, 8.27

Metro-Goldwyn-Mayer Studios, Inc. v Grokster, Ltd. (9th Cir 2004) 380 F3d 1154, vacated and remanded (2005) 545 US 913: §§1.16, 8.27

Metro-Goldwyn-Mayer Studios, Inc. v Grokster, Ltd. (CD Cal 2003) 259 F Supp 2d 1029, aff'd (9th Cir 2004) 380 F3d 1154, vacated and remanded (2005) 545 US 913: §8.27

Metro-Goldwyn-Mayer Studios, Inc. v Grokster, Ltd. (CD Cal 2003) 243 F Supp 2d 1073: §§19.8-19.9

Microsoft Corp. v AT&T Corp. (2007) 550 US 437, 167 L Ed 2d 737, 127 S Ct 1746: §2.2

Middlebrook v Anderson (ND Tex, Feb. 11, 2005, No. 3:04-CV-2294-D) 2005 US Dist Lexis 1976: §19.9

Middleton, U.S. v (9th Cir 2000) 231 F3d 1207: §18.12

Milkovich v Lorain Journal Co. (1990) 497 US 1, 111 L Ed 2d 1, 110 S Ct 2695: §20.15

Millennium Enters., Inc. v Millennium Music LP (D Or 1999) 33 F Supp 2d 907: §19.9

Miller v California (1973) 413 US 15, 37 L Ed 2d 419, 93 S Ct 2607: §20.16

Miller v Holzmann (D DC, Jan 17, 2007, No. 95-01231) 2007 US Dist Lexis 2987: §20A.28

Miller, In re (CCPA 1969) 418 F2d 1392: §2.3

Milliken v Meyer (1940) 311 US 457, 85 L Ed 278, 61 S Ct 339: §19.5

Moberg v 33T LLC (D Del 2009) 666 F Supp 2d 415: §1.8A

Moldo v Matsco, Inc. (In re Cybernetic Servs., Inc.) (BAP 9th Cir 1999) 239 BR 917, aff'd (9th Cir 2001) 252 F3d 1039, cert denied (2002) 534 US 1130: §16.28

Moldo v Matsco, Inc. (In re Cybernetic Servs., Inc.) (9th Cir 2001) 252 F3d 1039, cert denied (2002) 534 US 1130: §16.28

Monotype Imaging, Inc. v Bitstream Inc. (ND IL 2005) 376 F Supp 2d 877: §1.16A

Moore Bus. Forms v Ryu (5th Cir 1992) 960 F2d 486: §§3.53, 3.64

Morgan Stanley & Co. v Coleman (Parent) Holdings, Inc. (Fla App 2007) 955 So2d 1124: §20A.2

Moseley v V Secret Catalogue, Inc. (2003) 537 US 418, 155 L Ed 2d 1, 123 S Ct 1115: §3.65

Mrs. Fields Famous Brands, Inc., U.S. v (Mar. 6, 2003, Civ. Action No. CV205 JTG): §9.33

MySpace, Inc. v The Globe.com, Inc. (CD Cal, Feb. 27, 2007, No. CV 06-3391-RGK (JCx)) 2007 WL 1686966: §7.3

MySpace, Inc. v Wallace (CD Cal 2007) 498 F Supp 2d 1293: §17.22

N

NLRB v Bildisco & Bildisco (1984) 465 US 513, 79 L Ed 2d 482, 104 S Ct 1188: §12.12

Napster, Inc. Copyright Litig., In re (ND Cal 2006) 462 F Supp 2d 1060: §20A.28

Napster, Inc. Copyright Litig., In re (ND Cal 2002) 191 F Supp 2d 1087: §1.31

Narell v Freeman (9th Cir 1989) 872 F2d 907: §§1.2, 1.12

National Bellas Hess, Inc. v Department of Revenue (1967) 386 US 753, 18 L Ed 2d 505, 87 S Ct 1389, overruled in part by Quill Corp. v North Dakota (1992) 504 US 298, 119 L Ed 2d 91, 112 S Ct 1904: §10.23

National Council Against Health Fraud, Inc. v King Bio Pharms., Inc. (2003) 107 CA4th 1336, 133 CR2d 207: §17.9

National Fed'n of the Blind v Target Corp. (ND Cal 2007) 582 F Supp 2d 1185: §5.26

National Fed'n of the Blind v Target Corp. (ND Cal 2006) 452 F Supp 2d 946: §5.26

National Peregrine Inc. v Capitol Federal Sav. & Loan Ass'n (In re Peregrine Entertainment Ltd.) (CD Cal 1990) 116 BR 194: §16.27

Nedlloyd Lines B.V. v Superior Court (1992) 3 C4th 459, 11 CR2d 330: §§19.19-19.20

Nelson v United Technols. (1999) 74 CA4th 597, 88 CR2d 239: §4.3

Network Solutions Inc. v Umbro Int'l Inc. (Va 2000) 529 SE2d 80: §16.30

New Kids on the Block v News Am. Publ'g, Inc. (9th Cir 1992) 971 F2d 302: §3.72

New W. Corp. v NYM Co. (9th Cir 1979) 595 F2d 1194: §3.29

New York v Ferber (1982) 458 US 747, 73 L Ed 2d 1113, 102 S Ct 3348: §20.17

New York Times Co. v Sullivan (1964) 376 US 254, 11 L Ed 2d 686, 84 S Ct 710: §20.2

New York Times Co., Inc. v Tasini (2001) 533 US 483, 150 L Ed 2d 500, 121 S Ct 2381: §8.20

Newman v Quigg (Fed Cir 1989) 877 F2d 1575: §2.7

Newton v Diamond (9th Cir 2003) 349 F3d 591: §14.17

Nissan Motor Co. v Nissan Computer Corp. (9th Cir 2004) 378 F3d 1002: §3.65

North Am. Med. Corp. v Axiom Worldwide, Inc. (11th Cir 2008) 522 F3d 1211: §3.73

Nova Measuring Instruments Ltd. v Nanometrics, Inc. (ND Cal 2006) 417 F Supp 2d 1121: §20A.43

O

Odol-Werke Wien Gesellschaft M.B.H., Ex parte (Comm'r Pats 1956) 111 USPQ 286: §3.44

Official Unsecured Creditors' Comm. v Zenith Prods., Inc. (In re AEG Acquisition Corp.) (BAP 9th Cir 1993) 161 BR 50: §16.27

Offshore Rental Co. v Continental Oil Co. (1978) 22 C3d 157, 148 CR 867: §19.17

O'Grady v Superior Court (2006) 139 CA4th 1423, 44 CR3d 72: §20.2

Online Policy Group v Diebold, Inc. (ND Cal 2004) 337 F Supp 2d 1195: §1.37

Orifice, Daniel, Fitting Co. v Whalen (1962) 198 CA2d 791, 18 CR 659: §4.9

Owens-Corning Fiberglas Corp., In re (Fed Cir 1985) 774 F2d 1116: §3.77

Oyster Software, Inc. v Forms Processing, Inc. (ND Cal Dec. 6, 2001) 2001 US Dist Lexis 22520: §18.17

P

PDC Labs., Inc. v Hach Co. (CD Ill, Aug. 25, 2009, No. 09-1110) 2009 US Dist Lexis 75378: §7.4

PML N. Am. v Hartford Underwriters Ins. Co. (ED Mich, Dec. 20, 2006, No. 05-CV-70404-DT) 2006 US Dist Lexis 94456: §20A.28

Pagliero v Wallace China Co. (9th Cir 1952) 198 F2d 339: §3.82

Panavision Int'l v Toeppen (9th Cir 1998) 141 F3d 1316: §§19.7, 19.9

Parfums Givenchy v Drug Emporium (9th Cir 1994) 38 F3d 477, cert denied (1995) 514 US 1004: §1.23

Parker v Google (Ed Pa 2006) 422 F Supp 2d 492, aff'd (3d Cir 2007) 242 Fed Appx 833, cert denied (2008) ___ US ___, 169 L Ed 2d 834, 128 S Ct 1101: §§1.19, 1.32

PatentWizard, Inc. v Kinko's, Inc. (D SD 2001) 163 F Supp 2d 1069: §20.5

Payment Card Interchange Fee & Merchant Discount, In re (ED NY, Jan 12, 2007, MD 05-1720 (JG) (JO)) 2007 US Dist Lexis 2650 at *4: §20A.43

Payne v Elliot (1880) 54 C 339: §20.11

Pearson Educ. Inc. v Liao (SD NY, May 13, 07-Civ-2423 (SHS)) 2008 US Dist Lexis 39222: §1.23

Pebble Beach Co. v Caddy (9th Cir 2006) 453 F3d 1151: §§19.1-19.2, 19.4, 19.9-19.10

Pennoyer v Neff (1878) 95 US (5 Otto) 714: §19.5

Pension Comm. of Univ. of Montreal Pension Plan v Banc of Am. Sec. (SD NY, Jan. 15, 2010, No. 05 CIV 9016) 2010 US Dist Lexis 1839: §§20A.25, 20A.33

People v Direct Revenue, LLC (Sup Ct 2008) 862 NYS2d 816: §18.17

People ex rel Brown v PuriTec (2007) 153 CA4th 1524, 64 CR3d 270: §17.9

Peoples Telephone Co. v Hartford Fire Ins. Co. (SD Fla 1997) 36 F Supp 2d 1335: §20.37

PepsiCo, Inc. v Redmond (7th Cir 1995) 54 F3d 1262: §2.26

Perfect 10, Inc. v Amazon.com, Inc. (9th Cir 2007) 508 F3d 1146: §§1.6B, 1.15-1.16, 1.19

Perfect 10, Inc. v CCBill LLC (9th Cir 2007) 488 F3d 1102, cert denied (2007) ___ US ___, 169 L Ed 2d 553, 128 S Ct 709: §§1.30, 1.36

Perfect 10, Inc. v CCBill, LLC (CD Cal 2004) 340 F Supp 2d 1077: §§1.35, 20.6A, 20.6C

Perfect 10, Inc. v Cybernet Ventures, Inc. (CD Cal 2002) 213 F Supp 2d 1146: §§1.29-1.30, 1.42, 20.9

Perfect 10, Inc. v Visa Int'l Serv. Ass'n (9th Cir 2007) 494 F3d 788: §1.16A

Perfect 10, Inc. v Visa Int'l Serv. Ass'n (9th Cir 2007) 494 F3d 788, cert denied (2008) ___ US ___, 171 L Ed 2d 811, 128 S Ct 2871: §§1.13, 3.60

Perfect 10, Inc. v Visa Int'l Serv. Ass'n (ND Cal, Aug. 5, 2004, C04-0371JW) 2004 US Dist Lexis 15895: §1.42

PerfumeBay.com, Inc v Ebay, Inc. (9th Cir 2007) 506 F3d 1165: §3.65

Peskoff v Faber (D DC 2007) 244 FRD 54: §§20A.8, 20A.33

Petco Animal Supplies, Inc., In re (Nov. 8, 2004) No. 032-3221: §9.9A

Pharmatrak, Inc. Privacy Litig., In re (1st Cir 2003) 329 F3d 9: §§18.6, 18.8, 18.10

Pharmatrak, Inc. Privacy Litig., In re (D Mass 2003) 292 F Supp 2d 263: §9.15

Pharmatrak, Inc. Privacy Litig., In re (D Mass 2002) 220 F Supp 2d 4, rev'd on other grounds (1st Cir 2003) 329 F3d 9: §18.6

Phillips Petroleum Co. v Shutts (1985) 472 US 797, 86 L Ed 2d 628, 105 S Ct 2965: §19.15

Pietrylo v Hillstone Restaurant Group (D NJ, Sept. 25, 2009, No. 06-5754) 2009 US Dist Lexis 88702: §18.11

Planned Parenthood v American Coalition of Life Activists (9th Cir 2002) 290 F3d 1058: §20.15

Playboy Enters. v Netscape Communications Corp. (9th Cir 2004) 354 F3d 1020: §§3.60, 3.64, 3.72-3.74, 17.3

Playboy Enters., Inc. v Frena (MD Fla 1993) 839 F Supp 1552: §8.20

Playboy Enters., Inc. v Russ Hardenburgh, Inc. (ND Ohio 1997) 982 F Supp 503: §1.14

Playboy Enters., Inc. v Webbworld, Inc. (ND Tex 1997) 968 F Supp 1171, aff'd without opinion (5th Cir 1999) 168 F3d 486: §1.15

Playboy Enters., Inc. v Welles (9th Cir 2002) 279 F3d 796: §§3.71-3.72

Pollstar v Gigmania (ED Cal 2000) 170 F Supp 2d 974: §7.4

Porsche Cars N.A., Inc. v Porsche.net (4th Cir 2002) 302 F3d 248: §19.11

Powers v Thomas M. Cooley Law School (WD Mich, Sept. 21, 2006, No. 5:05-cv-117) 2006 US Dist Lexis 67706: §20A.38

ProCD, Inc. v Zeidenberg (7th Cir 1996) 86 F3d 1447: §7.2

Promatek Indus. Ltd. v Equitrac Corp. (7th Cir 2002) 300 F3d 808: §3.75

Providian Credit Card Cases, In re (2002) 96 CA4th 292, 116 CR2d 833: §2.37

Pueblo of Laguna v U.S. (2004) 60 Fed Cl 133: §20A.43

Q

Qualcomm Inc. v Broadcom Corp. (SD Cal 2007) 539 F Supp 2d 1214, aff'd in part and rev'd in part on other grounds (Fed Cir 2008) 548 F3d 1004: §20A.8

Qualcomm Inc. v Broadcom Corp. (SD Cal, Jan. 7, 2008, No. 05cv1958-B (BLM)) 2008 US Dist Lexis 911, aff'd in part and rev'd in part on other grounds (Fed Cir 2008) 548 F3d 1004: §20A.8

Qualitex Co. v Jacobson Prods. Co. (1995) 514 US 159, 131 L Ed 2d 248, 115 S Ct 1300: §3.80

Quill Corp. v North Dakota (1992) 504 US 298, 119 L Ed 2d 91, 112 S Ct 1904: §10.23

Quinby v WestLB AG (SD NY, Dec. 15, 2005, No. 04-CIV-7406) 2005 US Dist Lexis 35583: §20A.27

Quinton Instruments Co. v Impra, Inc. (In re Mahurkar Double Lumen Hemodialysis Cathetar Patent Litig.) (Fed Cir 1995) 71 F3d 1573: §2.13

Quon v Arch Wireless (9th Cir 2008) 529 F3d 892, cert granted sub nom City of Ontario v Quon (2009) ___ US ___, 175 L Ed 2d 617, 130 S Ct 1011: §9.15

R

Rambus, Inc. v Infineon Tech. AG (ED Va 2004) 220 FRD 264: §20A.4

RealNetworks, Inc. v Streambox, Inc. (WD Wa, Jan. 18, 2000, No. C99-2070P) 2000 US Dist Lexis 1889: §1.25

Recording Indus. Ass'n v Charter Communications, Inc. (In re Charter Communications, Inc.) (8th Cir 2005) 393 F3d 771: §§1.29, 1.41

Recording Indus. Ass'n v Diamond Multimedia (9th Cir 1999) 180 F3d 1072: §8.27

Recording Indus. Ass'n v Verizon Internet Servs., Inc. (DC Cir 2003) 351 F3d 1229, cert denied (2004) 543 US 924: §§1.29, 1.41

Register.com, Inc. v Verio, Inc. (2d Cir 2004) 356 F3d 393: §7.4

Register.com, Inc. v Verio, Inc. (SD NY 2000) 126 F Supp 2d 238, aff'd (2004) 356 F3d 393: §§18.19-18.20

Reid, State v (NJ 2008) 945 A2d 26: §9.6

Religious Technol. Ctr. v F.A.C.T.Net, Inc. (D Colo 1995) 901 F Supp 1519: §2.35

Religious Technol. Ctr. v Lerma (ED Va 1995) 897 F Supp 260: §2.35

Religious Technol. Ctr. v Netcom On-Line Communication Servs., Inc. (ND Cal 1995) 923 F Supp 1231: §§1.19-1.21, 2.20, 2.35

Religious Technol. Ctr. v Netcom On-Line Communication Servs., Inc. (ND Cal 1995) 907 F Supp 1361: §§1.14-1.15, 1.31

Reno v ACLU (1997) 521 US 844, 138 L Ed 2d 874, 117 S Ct 2329: §§20.5, 20.18

Rescuecom Corp. v Google, Inc. (2d Cir 2009) 562 F3d 123: §3.73

Retail Sys., Inc. v CNA Ins. Cos. (Minn App 1991) 469 NW2d 735: §20.36

Rex Chainbelt Inc.v Borg-Warner Corp. (7th Cir 1973) 477 F2d 481: §2.14

Rhoads Indus., Inc. v Building Materials Corp. of Am. (ED Pa 2008) 254 FRD 216: §20A.44A

Rickard v Auto Publisher, Inc. (11th Cir 1984) 735 F2d 450: §3.31

Rio Props., Inc. v Rio Int'l Interlink (9th Cir 2002) 284 F3d 1007: §19.2

Rocker Mgmt. LLC v John Does 1-20 (ND Cal, May 29, 2003, No. 03-003 3 CRB) 2003 US Dist Lexis 16277: §20.3

Roberts v Boyd, WIPO Case No. D2000-0210: §20.30

Roberts, Julia Fiona v Russell Boyd, WIPO Case No. D2000-210: §20.30

Roe v Wade (1973) 410 US 113, 35 L Ed 2d 147, 93 S Ct 705: §9.7

Rolley, Inc. v Younghusband (9th Cir 1953) 204 F2d 209: §3.30

Roman Cleanser Co., In re (Bankr ED Mich 1984) 43 BR 940, aff'd (6th Cir 1986) 802 F2d 207: §16.29

Roman Cleanser Co., In re (6th Cir 1986) 802 F2d 207: §16.29

Rossi v Motion Picture Ass'n (9th Cir 2004) 391 F3d 1000, cert denied (2005) 544 US 1018: §1.37

Roth v U.S. (1957) 354 US 476, 1 L Ed 2d 1498, 77 S Ct 1304: §20.16

Ruiz v Gap, Inc. (ND Cal 2008) 540 F Supp 2d 1121: §9.17

S

SMC Promotions, Inc. v SMC Promotions (CD Cal 2005) 355 F Supp 2d 1127: §17.3

Salcedo, U.S. v (4th Cir 2006) 189 Fed Appx 197: §18.7A

Save Venice NY, Inc., In re (Fed Cir 2001) 259 F3d 1346: §3.32

Savin Corp. v Savin Group (2d Cir 2004) 391 F3d 439: §3.65

Schenk v U.S. (1919) 249 US 47, 63 L Ed 470, 39 S Ct 247: §20.15

Schwartz v Comcast Corp. (3d Cir 2007) 256 Fed Appx 515: §7.4

Seagate Technol., LLC, In re (Fed Cir 2007) 497 F3d 1360: §2.17A

Sears Holdings Mgmt. Corp., In re (June 4, 2009) FTC File No. 082 3099: §9.6

Sega Enters. Ltd. v Accolade, Inc. (9th Cir 1992) 977 F2d 1510: §1.19

Sega Enters. Ltd. v MAPHIA (ND Cal 1996) 948 F Supp 923: §§1.15, 8.20

Sega Enters. Ltd. v Sabella (ND Cal, Dec. 18, 1996, No. C 93-04260 CW) 1996 US Dist Lexis 20470: §1.15

Sengoku Works Ltd. v RMC Int'l, Ltd. (9th Cir1996) 96 F3d 1217, cert denied (1997) 521 US 1103: §3.29

Shaffer v Heitner (1977) 433 US 186, 53 L Ed 2d 683, 97 S Ct 2569: §19.6

Shamrock Foods Co. v Gast (D Ariz 2008) 535 F Supp 2d 962: §18.7

Shapiro, Bernstein & Co. v H.L. Green Co. (2d Cir 1963) 316 F2d 304: §§1.13, 1.16

Shaw v Lindheim (9th Cir 1990) 919 F2d 1353: §1.12

Shields v Zuccarini (3rd Cir 2001) 254 F3d 476: §3.22

Shisler v Sanfer Sports Cars, Inc. (2006) 146 CA4th 1254, 53 CR3d 335: §19.10

Shulman v Group W Prods., Inc. (1998) 18 C4th 200, 74 CR2d 843: §9.17

Shurgard Storage Ctrs., Inc. v Safeguard Self Storage, Inc. (WD Wa 2000) 119 F Supp 2d 1121: §§18.3, 18.7

Shutts, In re (TTAB 1983) 217 USPQ 363: §3.28

Sicilia Di R. Biebow & Co. v Cox (5th Cir 1984) 732 F2d 417: §3.82

Silvestri v General Motors Corp. (4th Cir 2001) 271 F3d 583: §§20A.21-20A.22

Sims v Lakeside Sch. (WD Wash, Sept. 20, 2007, No. C06-1412RSM) 2007 US Dist Lexis 69568: §20A.5

Sinclair v Aquarius Electronics, Inc. (1974) 42 CA3d 216, 116 CR 654: §§2.24, 2.35

Small, U.S. v (3d Cir 2003) 333 F3d 425, rev'd on other grounds (2005) 541 US 385: §21.5

Smith v Department of Employment (1976) 62 CA3d 206, 132 CR 874: §4.14

Smith v Maryland (1979) 442 US 735, 61 L Ed 2d 220, 99 S Ct 2577: §9.7

Smith, Valentino & Smith, Inc. v Superior Court (1976) 17 C3d 491, 131 CR 374: §19.12

Snowney v Harrah's Entertainment, Inc. (2005) 35 C4th 1054, 29 CR3d 33: §19.8

Sony Computer Entertainment Am. Inc. v GameMasters, Inc. (ND Cal 1999) 87 F Supp 2d 976: §1.25

Sony Computer Entertainment Am., Inc. v Filipiak (ND CA 2006: §1.27

Sony Corp. v Universal City Studios, Inc. (1984) 464 US 417, 78 L Ed 2d 574, 104 S Ct 774: §§1.16, 1.18, 8.27

Sony Music Entertainment v Does (SD NY 2004) 326 F Supp 2d 556: §20.24

Sotelo v DirectRevenue, LLC (ND Ill 2005) 384 F Supp 2d 1219: §18.20A

Southdale Kay-Bee Toy, Inc. & KBkids.com LLC, U.S. v (July 26, 2000) FTC File No. 0023115: §10.16

Southland Corp. v Schubert (CD Cal 1968) 297 F Supp 477: §3.31

Southwest Airlines Co. v Boardfirst, LLC (ND Tex, Sept. 12, 2007, No. 3: 06-CV-0891-B) 2007 US Dist Lexis 96230: §7.4

Soverain Software, LLC v Amazon.com, Inc. (ED Tex 2005) 383 F Supp 2d 904: §2.10

Specht v Communications Netscape Communications Corp. (2d Cir 2002) 306 F3d 17: §7.4

Specht v Netscape Communications Corp. (2d Cir 2002) 306 F3d 17: §7.4

Specht v Netscape Communications Corp. (SD NY 2001) 150 F Supp 2d 585, aff'd (2d Cir 2002) 306 F3d 17: §7.14

Sports Auth., Inc. v Abercrombie & Fitch (ED Mich 1997) 965 F Supp 925: §3.51

Springsteen v Burgar, WIPO Case No. D2000-1532: §20.30

St. Paul Fire & Marine Ins. Co. v National Computer Sys., Inc. (Minn App 1992) 490 NW2d 626: §20.37

Standard Oil Co. v FTC (9th Cir 1978) 577 F2d 653: §17.4

Standard Process, Inc. v Banks (ED Wis 2008) 554 F Supp 2d 866: §3.73

State v Reid (NJ 2008) 945 A2d 26: §9.6

State Auto Prop. & Cas. Ins. Co. v Midwest Computers & More (WD Okla 2001) 147 F Supp 2d 1113: §20.38

State Farm Fire & Cas. Co. v Steinberg (11th Cir 2004) 393 F3d 1226: §20.39

State St. Bank & Trust Co. v Signature Fin. Group (1998) 149 F3d 1368, cert denied (1999) 525 US 1093: §§2.1, 2.18-2.19

Step-Saver Data Sys. v Wyse Technol. (3d Cir 1991) 939 F2d 91: §§7.2, 7.14

Stevens v Publicis (App Div 2008) 854 NYS2d 690: §7.6

Stevenson v Union Pac. R.R. (8th Cir 2004) 354 F3d 739: §20A.21

Stilwell Dev., Inc. v Chen (CD Cal 1989) 11 USPQ2d 1328: §2.36

Storage Technol. Corp. v Custom Hardware Eng'g & Consulting, Inc. (Fed Cir 2005) 421 F3d 1307: §§1.16B, 1.24

Storus Corp. v Aroa Mktg., Inc. (ND Cal 2008) 87 USPQ2D 1032: §3.73

Stratton Oakmont v Prodigy Servs., Inc. (Sup Ct 1995) 1995 NY Misc Lexis 229: §20.4

SuccessFactors, Inc. v Softscape, Inc. (ND Cal 2008) 544 F Supp 2d 975: §18.3

Supoena Duces Tecum to AOL, LLC, In re (ED Va 2008) 550 F Supp 2d 606: §20A.5

T

TBG Ins. Servs. v Superior Court (2002) 96 CA4th 443, 117 CR2d 155: §9.16

TMI, Inc. v Maxwell (5th Cir 2004) 368 F3d 433: §20.29

Taco Cabana Int'l, Inc. v Two Pesos, Inc. (5th Cir 1991) 932 F2d 1113, aff'd (1992) 505 US 763: §3.53

Talley v California (1960) 362 US 60, 4 L Ed 2d 559, 80 S Ct 536: §20.24

Taubman Co. v Webfeats (6th Cir 2003) 319 F3d 770: §20.29

Theofel v Farey-Jones (9th Cir 2003) 359 F3d 1066: §18.11

Theofel v Farey-Jones (9th Cir 2003) 341 F3d 978, reprinted as amended (9th Cir 2004) 359 F3d 1066, cert denied (2004) 166 L Ed 2d 17: §18.11

Therapeutic Research Faculty v NBTY, Inc. (ED Cal 2007) 488 F Supp 2d 991: §§2.22, 18.5, 18.11, 18.16

Thomas, U.S. v (6th Cir 1996) 74 F3d 701: §20.16

Thompson v Handa-Lopez (WD Tex 1998) 998 F Supp 738: §19.12

Thompson Med. Co. (1984) 104 FTC 648, aff'd (DC Cir 1986) 791 F2d 189, cert denied (1987) 479 US 1086: §17.4

Thriftimart, Inc. v Scot Lad Foods, Inc. (TTAB 1980) 207 USPQ 330: §3.40

Thrifty-Tel, Inc. v Bezenek (1996) 46 CA4th 1559, 54 CR2d 468: §18.21A

Ticketmaster Corp. v Tickets.com, Inc. (CD Cal 2000) 54 USPQ2d 1344: §8.16

Ticketmaster Corp. v Tickets.com, Inc. (CD Cal, Aug. 10, 2000, CV99-7654 HLH) 2000 US Dist Lexis 12987, aff'd without opinion (9th Cir 2001) 248 F3d 1173: §§18.17, 18.21

Ticketmaster Corp. v Tickets.com, Inc. (CD Cal, Mar. 7, 2003, CV99-7654 HLH) 2003 US Dist Lexis 6483: §7.4

Ticketmaster Corp. v Tickets.com, Inc. (CD Cal, Mar. 27, 2000, CV99-7654 HLH) 2000 US Dist Lexis 4553: §7.4

Ticketmaster Corp. v Tickets.com, Inc. (CD Cal, Mar. 7, 2003, CV99-7654 HLH) 2003 US Dist Lexis 6484, *12, aff'd (9th Cir 2005) 127 Fed Appx 346 (unpublished opinion): §18.21

Ticketmaster LLC v RMG Technols., Inc. (CD Cal 2007) 507 F Supp 2d 1096: §§1.19, 7.4

Tieberg v Unemployment Ins. Appeals Bd. (1970) 2 C3d 943, 88 CR 175: §4.14

Tiffany Inc. v eBay, Inc. (SD NY 2008) 576 F Supp 2d 463: §§3.60, 3.72

Times Mirror Magazines Inc. v Las Vegas Sports News (3d Cir 2000) 212 F3d 157: §3.65

Together Dev. Corp., In re (Bankr D Mass 1998) 227 BR 439, aff'd (D Mass 2000) 255 BR 606: §16.29

Toshiba Am. Electronic Components, Inc. v Superior Court (2004) 124 CA4th 762, 21 CR3d 532: §20A.49

Toys R Us, Inc. v Akkaoui (ND Cal, Oct. 29, 1996, No. C 96-3381) 1996 US Dist Lexis 17090: §3.65

Toys R Us, Inc. Privacy Litig., In re (ND Cal, Oct. 9, 2001) 2001 US Dist Lexis 16947: §18.9

Toysrus.com, LLC & Toysrus.com, Inc., U.S. v (July 26, 2000) FTC File No. 0023008: §10.16

Traditional Cat Ass'n v Gilbreath (2004) 118 CA4th 392, 13 CR3d 353: §20.2

TrafFix Devices, Inc. v Marketing Displays, Inc. (2001) 532 US 23, 149 L Ed 2d 164, 121 S Ct 1255: §3.80

Transportation Design & Technol., Inc., In re (Bankr SD Cal 1985) 48 BR 635: §16.28

Treiber & Straub, Inc. v UPS, Inc. (7th Cir 2007) 474 F3d 379: §7.4

Treppel v Biovail Corp. (SD NY 2006) 233 FRD 363: §20A.27

Treu v Garrett Corp. (1968) 264 CA2d 432, 70 CR 284: §4.9

Triad Sys. Corp. v Southeastern Express Co. (9th Cir 1995) 64 F3d 1330: §1.16B

Turnbull v American Broadcasting Cos. (CD Cal, 2004) 2004 US Dist Lexis 24351: §9.21A

Turner v Anheuser-Busch (1994) 7 C4th 1238, 32 CR2d 223: §4.5

Two Pesos, Inc. v Taco Cabana, Inc. (1992) 505 US 763, 120 L Ed 2d 615, 112 S Ct 2753: §§3.28, 3.77, 3.79, 3.84, 3.86

U

U.S. v _____ (*see* name of defendant)

U.S. Tobacco Co., In re (TTAB 1986) 1 USPQ2d 1502: §3.27

UEJF et La Licra v Yahoo! Inc. et Yahoo France, Tribunal de Grande Instance de Paris (Nov. 20, 2000): §21.3

UMG Recordings, Inc. v Lindor (ED NY 2007) 531 F Supp 2d 453: §8.28

UMG Recordings, Inc. v MP3.Com Inc. (SD NY 2000) 92 F Supp 2d 349: §8.27

UMG Recordings, Inc. v Veoh Networks, Inc. (CD Cal 2009) 665 F Supp 2d 1099: §1.35

UMG Recordings, Inc., U.S. v (Feb. 18, 2004, Civ Action No. CV-04-1050 JFW): §9.33

Universal City Studios, Inc. v Reimerdes (SD NY 2000) 111 F Supp 2d 294, aff'd sub nom Universal Studios, Inc. v Corley (2d

Cir 2001) 273 F3d 429: §§1.25-1.26

Universal Communication Sys. v Lycos, Inc. (1st Cir 2007) 478 F3d 413: §§20.6-20.7

Urecal Corp. v Masters (ND Ill 1976) 413 F Supp 873: §3.51

Urofsky v Gilmore (4th Cir 2000) 216 F3d 401, cert denied (2001) 531 US 1070: §20.23

V

VL Sys., Inc. v Unisen, Inc. (2007) 152 CA4th 708, 61 CR3d 818.: §2.26

ValueClick, Inc., U.S. v (CD Cal 2008) Case No. CV08-01711 MMM (RZx): §17.22

Varian Med. Sys., Inc. v Delfino (2003) 113 CA4th 273, 6 CR3d 325, rev'd on other grounds (2005) 35 C4th 180, 25 CR3d 298: §20.3

Vas-Cath, Inc. v Mahurkar (Fed Cir 1991) 935 F2d 1555: §2.11

Vault Corp. v Quaid Software Ltd. (5th Cir 1988) 847 F2d 255: §7.2

Venture Tape Corp. v McGills Glass Warehouse (1st Cir 2008) 540 F3d 56: §3.73

Verisign Secs. Litig., Inc., In re (ND Cal, Mar. 10, 2004, No. C 02-02270 JW) 2004 US Dist Lexis 22467: §20A.43

Verizon Internet Servs., Inc., In re (D DC 2003) 240 F Supp 2d 24: §1.42

Vernor v Autodesk, Inc. (WD Wash 2009) 93 USPQ2d 1336: §1.16B

Vernor v Autodesk, Inc. (WD Wash 2008) 555 F Supp 2d 1164: §1.23

Viacom Int'l Inc. v YouTube Inc. (SD NY 2008) 253 FRD 256: §2.22A

Viacom Int'l, Inc. v YouTube, Inc. (SD NY 2008) 540 F Supp 2d 461: §1.17

Victor Stanley, Inc. v Creative Pipe, Inc. (D Md 2008) 250 FRD 251: §20A.44A

Video Pipeline v Buena Vista Home Entertainment, Inc. (NJ 2002) 192 F Supp 2d 321, aff'd (3d Cir 2003) 342 F3d 191, cert denied (2004) 540 US 1178: §§1.23, 8.20

Virtual Works, Inc. v Volkswagen of Am., Inc. (4th Cir 2001) 238 F3d 264: §3.23

Voicenet Communications, Inc. v Corbett (ED Pa, Aug. 30, 2006, No. 04-1318) 2006 US Dist Lexis 61916: §20.7

Volkswagenwerk Aktiengesellschaft v Church (9th Cir 1969) 411 F2d 350: §3.68

W

W.L. Gore & Assocs., Inc. v Garlock, Inc. (Fed Cir 1983) 721 F2d 1540, cert denied (1984) 469 US 851: §§2.2, 2.11

Wal-Mart Stores v Samara Bros., Inc. (2000) 529 US 205, 146 L Ed 2d 182, 120 S Ct 1339: §§3.77, 3.85

Walker Process Equipment Inc., In re (Comm'r Pats 1954) 102 USPQ 443, aff'd (CCPA 1956) 233 F2d 329: §3.47

Wall Data Inc. v Los Angeles County Sheriff's Dep't (9th Cir 2006) 447 F3d 769: §§1.16B, 12.4A

Wands, In re (Fed Cir 1988) 858 F2d 731: §2.11

Warner, Mark, 2001 v Mike Larson, Nat'l Arbitration Forum Case Case No. FA0009000095746, Nov. 15: §20.30

WarnerVision Entertainment v Empire of Carolina, Inc. (2d Cir 1996) 101 F3d 259: §3.35

Washington Mut. Bank, FA v Superior Court (2001) 24 C4th 906, 103 CR2d 320: §§19.16-19.17, 19.20

Watkins v L.M. Berry & Co. (11th Cir 1983) 704 F2d 577: §18.11A

Weaver, U.S. v (CD Ill 2009) 636 F Supp 2d 769: §18.11

Web Communications, In re (TTAB 1998) 49 USPQ2d 1478: §3.28

Wells Fargo & Co. v Lundeen & Assocs. (TTAB 1991) 20 USPQ 2d 1156: §3.51

Wembley, Inc., Ex parte (Comm'r Pats 1956) 111 USPQ 386: §3.27

Westcoat v Bayer CropScience LP (ED Mo, Nov. 1, 2006, No. 4:06-cv-01529-ERW) 2006 US Dist Lexis 79756: §§20A.24, 20A.26

Whyte v Schlage Lock Co. (2002) 101 CA4th 1443, 125 CR2d 277: §2.26

Wilbanks v Wolk (2004) 121 CA4th 883, 17 CR3d 497: §20.25

William A. Gross Constr. Assocs., Inc. v American Mfrs. Mut. Ins. Co. (SD NY 2009) 256 FRD 134: §20A.4

Williams v Sprint/United Mgmt. Co. (D Kan 2005) 230 FRD 640: §§20A.36, 20A.43

Williams-Sonoma, Inc. v FriendFinder, Inc. (ND Cal, April 17, 2007, No. C 06-06572 JSW) 2007 US Dist Lexis 31299: §19.2

Winklevoss Consultants, Inc. v Federal Ins. Co. (ND Ill 1998) 991 F Supp 1024: §20.39

Wise, U.S. v (9th Cir 1977) 550 F2d 1180: §§1.16B, 1.23

World-Wide Volkswagen v Woodson (1980) 444 US 286, 62 L Ed 2d 490, 100 S Ct 559: §§19.6-19.7, 19.10

Worldwide Church of God v Philadelphia Church of God, Inc. (9th Cir 2000) 227 F3d 1110, cert denied (2001) 532 US 958: §1.19

Worth v Selchow & Righter Co. (9th Cir 1987) 827 F2d 569, cert denied (1988) 485 US 977: §1.2

X

Xanga.com, Inc., U.S. v (Sept. 7, 2006, Civ Action No. 06-CIV-6853 SHS FTC File No. 062-3073: §9.33

Y

Yahoo!, Inc. v La Ligue Contre le Racisme et L'Antisemitisme (9th Cir 2006) 433 F3d 1199: §21.5

Yahoo!, Inc. v La Ligue Contre le Racisme et L'Antisemitisme (9th Cir 2005) 399 F3d 1010: §21.5

Yahoo!, Inc. v La Ligue Contre le Racisme et L'Antisemitisme (9th Cir 2004) 379 F3d 1120: §21.5

Yahoo!, Inc. v La Ligue Contre le Racisme et L'Antisemitisme (9th Cir 2004) 379 F3d 1120, rehearing en banc granted (Feb. 10, 2005, No. 01-17424) 399 F3d 1010: §19.10

Yahoo!, Inc. v La Ligue Contre le Racisme et L'Antisemitisme (ND Cal 2001) 169 F Supp 2d 1181, rev'd and remanded with instructions to dismiss without prejudice (9th Cir 2006) 433 F3d 1199: §21.5

Yahoo!, Inc. v Yahooahtos.com (ED Va, Aug. 8, 2006, No. 1:05cv1441) 2006 US Dist Lexis 54902: §3.22

Yang, U.S. v (6th Cir 2002) 281 F3d 534, cert denied (2003) 537 US 1170: §2.38

Yousef Jameel v Dow Jones & Co., Inc. (2005) EWCA Civ 75: §21.4

Z

Zacchini v Scripps-Howard Broadcasting Co. (1977) 433 US 562, 53 L Ed 2d 965, 97 S Ct 2849: §20.9

Zango, Inc. v Kaspersky Lab, Inc. (9th Cir 2009) 568 F3d 1169: §20.6D

Zeran v AOL (4th Cir 1997) 129 F3d 327, cert denied (1998) 524 US 937: §20.6

Zheng v Yahoo! Inc. (ND Cal, Dec. 2, 2009, No. C-08-1068 MMC) 2009 US Dist Lexis 111886: §21.3

Ziegler, U.S. v (9th Cir 2007) *474* F3d 1184: §9.15

Zippo Mfg. v Zippo Dot Com (WD Pa 1997) 952 F Supp 1119: §§19.1-19.2, 19.7, 19.10

Zirco Corp. v American Tel. & Tel. (TTAB 1991) 21 USPQ2d 1542: §3.35

Zubulake v UBS Warburg LLC (SD NY 2004) 229 FRD 422: §20A.25

Zubulake v UBS Warburg LLC (SD NY 2003) 220 FRD 212: §§20A.3, 20A.19, 20A.21-20A.22, 20A.25-20A.26

Zubulake v UBS Warburg LLC (SD NY 2003) 220 FRD 422: §20A.25

Zubulake v UBS Warburg LLC (SD NY 2003) 216 FRD 280: §20A.49

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/Table of References

Table of References

Advising California Employers and Employees (Cal CEB 2005): §§4.1, 4.11-4.14

Advising California Partnerships (3d ed Cal CEB 1999): §16.2

Ballon, Ian C. E-Commerce & Internet Law: Treatise With Forms. Eagan, Minn., West, 2d ed 2009: §7.1

Black's Law Dictionary. St. Paul, Minn., West Publishing, 6th ed 1990: §20.36

California Business Litigation (Cal CEB 2002): §§1.1, 2.1, 2.15, 3.26, 3.60, 9.17, 9.27

California Civil Discovery Practice (4th ed Cal CEB 2006): §§20A.1, 20A.9, 20A.13, 20A.29-20A.30

California Mortgages, Deeds of Trust, and Foreclosure Litigation (4th ed Cal CEB 2009): §16.21

Chisum, Donald S. Patents: A Treatise on the Law of Patentability, Validity and Infringement. New York, Matthew Bender, 2003: §2.1

Fields, Robert J. Understanding and Managing Sales and Use Tax. Chicago, CCH, 5th ed 2001: §10.22

Financing and Protecting California Businesses (Cal CEB 2006): §§4.6, 16.1-16.2, 16.5, 16.8-16.9, 16.15-16.16, 16.22, 16.34

Forming and Operating California Limited Liability Companies (2d ed Cal CEB 2007): §16.2

McCarthy, J. Thomas. McCarthy on Trademarks and Unfair Competition. Deerfield, Ill, Clark Boardman Callaghan, 4th ed 1996: §§3.26, 3.81-3.82, 3.85

Nimmer, Melville B., & David Nimmer. Nimmer on Copyright: A Treatise on the Law of Literary, Musical and Artistic Property, and the Protection of Ideas. New York, Matthew Bender, 1978-: §§1.1, 1.18, 8.20

Organizing Corporations in California (3d ed Cal CEB 2001): §16.2

Sales and Mergers of California Businesses (Cal CEB 2002): §§22.1, 22.3, 22.16

Sales and Use Taxation of E-Commerce: State Tax Administrator's Current Thinking with CCH Commentary (CCH, Chicago, 2000): §10.22

Secured Transactions in California Commercial Law Practice (2d ed Cal CEB 2001): §§16.26, 16.32

Trade Secrets Practice in California (2d ed Cal CEB 1996): §§2.20, 2.22-2.26, 2.34-2.38, 4.6-4.7, 16.31

United States Patent and Trademark Office. A Guide to Filing a Non-Provisional (Utility) Patent Application. Alexandria, Va., June 2005: §2.10

——. Manual for Patent Examining Procedure. Alexandria, Va., 8th ed rev August 2006: §§2.3, 2.8, 2.18

——. Trademark Manual of Examining Procedure. Alexandria, Va., 4th ed April 2005 (TMEP): §§3.27, 3.32, 3.35, 3.37-3.38, 3.43-3.44, 3.50-3.51, 3.77

West Group. Restatement (Second) of Conflict of Laws. Eagan, Minn. 1971: §19.20

——. Restatement (Second) of Torts. Eagan, Minn., 1977: §§20.2-20.3, 20.11, 20.28

——. Restatement (Third) of Foreign Relations Law of the United States, Eagan, Minn., 1987: §§21.3-21.5

——. Restatement (Third) of Unfair Competition. Eagan, Minn., 1993: §2.21

——. Restatement (Third) of Unfair Competition. Eagan, Minn., 1995: §3.82

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/Table of Forms

Table of Forms

Advisory board letter agreement, 4.23

Agreement for transfer and assignment of intellectual property, 5.3

Banner advertising agreement, 17.32

Basic technical support exhibit, 6.49

Choice-of-forum clause, 19.13

Choice-of-law clause, 19.22

Co-branding agreement, 11.7

Co-location agreement, 6.19

Confidentiality agreement, 2.33

Confidentiality and Invention Assignment Agreement, 4.11

Convertible promissory note, 16.35

Copyright

Assignment, 1.10

U.S. Copyright Office Cover sheet, 1.11

Digital reprint rights license, 14.14

Domain names

Assignment agreement, 22.19

Purchase agreement, 3.8

Endorsement agreement, 14.10

Evaluation license agreement, 8.11

Exclusivity clause, 12.10

Hosting services agreement, 6.12

Independent contractors

Consulting agreement, 4.19

Nondisclosure agreement, 4.20

Intellectual property

Due diligence report re, 22.15

Representations and warranties re, 22.17

Interactive marketing agreement, 17.36

Internet advertising agreement, 17.34

Legal hold letter to client, 20A.24

Linking agreement, 8.18

Litigation hold letter to opponent, 20A.26

Loan agreement, 16.24

Offer letter to prospective employee, 4.5

Online beta user evaluation agreement, 8.7

Online end-user software license agreement, 8.5

Online software developer toolkit license agreement, 8.13

Open source software license agreement, 8.9

Patents

Assignment, 2.16

U.S. Patent and Trademark Office cover sheet, 2.17

Privacy policy

Basic website privacy policy, 9.44

Commercial website privacy policy, 9.46

Promissory note, 16.25

Sample clauses re payment of subscription fees, 10.15

Security agreement (intellectual property), 16.33

Short form service level agreement, 6.37

Software development agreement, 13.3

Software license agreement, 12.7

Software test and evaluation agreement, 13.5

Source code escrow agreement, 15.2

Still photograph license, 14.12

Strategic alliance

Agreement for strategic alliance, 11.5

Letter of intent re, 11.3

Streaming video license, 14.16

Technical support and maintenance agreement, 6.46

Term sheet for preferred stock financing, 16.10

Trademark

Assignment, 3.58

Cease and desist letter, 3.70

Guidelines, 3.55

License agreement, 3.56

U.S. Patent and Trademark Office cover sheet, 3.59

Trade secrets and confidential information protection, company policy on, 2.32

Uniform Domain Name Dispute Resolution Policy (UDRP)

Complaint, 3.18

Response, 3.20

Website development agreement, 5.25

Website hosting service level agreement, 6.39

Website terms of use, 8.3

© The Regents of the University of California

Source: Business Law/Internet Law and Practice in California/Index

Index

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

References are to chapter section numbers

The symbol "" after a section number indicates that a form appears in the section.

Abandonment of Trademark. See Trademarks, Service Marks, and Trade Names

Acquisitions and Sales of Internet-Based Businesses

Domain name ownership change, domain name assignment agreement, 22.18, 22.19

Due diligence procedures for intellectual property

Generally, 22.1, 22.3

Advance preparation by seller, 22.8

Analyzing information received during due diligence investigation, 22.10

Buyer's due diligence report, 22.9, 22.14, 22.15

Checklist, 22.5, 22.12, 22.13

Confidentiality agreement, 22.4

Disposition of information after due diligence, 22.11

Open source software, 22.13A-22.13B

Responding to due diligence request, 22.7

Seller's internal response team, 22.6

Open source software. See **Open Source Software**

Preliminary issues before entering negotiations, 22.1

Representations and warranties, intellectual property in purchase agreement, 22.1, 22.3, 22.16, 22.17

Addresses

CAN-SPAM Act, valid postal address requirement under, 17.14, 17.17

Website addresses. See **Websites (Generally)**

ADR. See Alternative Dispute Resolution (ADR)

Advertising

See also **Marketing**

Generally, 17.1

Advertainment, 17.30

Advertising and Marketing on the Internet: Rules of the Road (FTC publication), 17.5

Agreements, generally, 17.30

Applicable laws, generally, 17.2

Attorneys advertising services on Internet, effect of ethics rules on, 17.10A-17.10D

Banner ads. See **Banner Advertising**

California Department of Consumer Affairs (DCA), regulation by, 17.9

CAN-SPAM Act, identification as advertisement, 17.14-17.15, 17.18, 17.20

Co-branding arrangements, 17.1

Cookies, targeted advertising through use of, 18.9

E-mail

Mass e-mail messages, 17.1

Unsolicited e-mail (spam). See **Spam E-Mail**

False or misleading advertising, laws prohibiting

Generally, 17.9

CAN-SPAM act, deceptive advertising provisions under, 17.19

Federal Trade Commission Act, liability for false or deceptive advertising under, 17.4, 17.6

Injunctive relief against false or misleading advertising, 17.6, 17.9

Lanham Act, 17.3

Federal Trade Commission Act, 17.4, 17.6

Form of Internet advertising agreement, 17.34

Insurance policy provision for advertising liability coverage, 20.41

Lanham Act, advertising provisions, 17.3

Linking arrangements. See **Linking Arrangements**

Metatags, 17.1

Pop-up ads, 17.1

Portal agreements, 17.35, 17.36

Regulation of, 17.1

Service directories or referral sites, 17.33

State laws, generally, 17.8

Telephone, Internet, and catalog sales, laws regulating, 17.8, 17.10

Types of, 17.1

Advisory Boards

Generally, 4.22

Sample form, advisory board letter agreement, 4.23

Adware, 9.6A, 9.9B

Affidavits and Declarations

Trademark, affidavit for renewing registration of, 3.52

Agents and Agency

Digital Millennium Copyright Act (DMCA), ISP designating agent to receive notification of copyright infringement as safe harbor requirement under, 1.34

Agreements. See Contracts

Alliances. See Strategic Alliances

Alternative Dispute Resolution (ADR)

See also **Arbitration**

International business transactions, ADR for, 21.20

Software license agreements, ADR provisions in, 8.4

World Intellectual Property Organization. See **World Intellectual Property Organization (WIPO)**

Ambiguities

Website development agreement's ambiguous language construed against drafter, 5.5

Amendments and Modifications

Copyright law, amendment of. See **Digital Millennium Copyright Act (DMCA)**

Electronic agreements, modification of terms and conditions, 7.14

Software license modifications, 7.4

Trademarks. See **Trademarks, Service Marks, and Trade Names**

Website developer, license grants permitting modification of company-furnished content by, 5.17, 5.26

Angel Investors, 16.3, 16.6, 16.34

Anticybersquatting Consumer Protection Act (ACPA)

See also **Cybersquatters**

Domain names. See **Domain Names**

Trademarks, protection for, 3.62

Antidilution

Term sheet for preferred stock financing, antidilution provision in, 16.10

Anti-Phishing Act of 2005, 3.63, 9.6C

Anti-SLAPP Statute

Motion to strike complaint under California's Anti-SLAPP statute, 20.25

Appeals

Domain name infringement claim, appealing arbitration panel's decision, 3.21

Patent, appeal of rejected application, 2.10

Trademark, appealing denial of registration, 3.50

Application Service Provider (ASP)

Service level agreements, ASP's responsibility for software accessibility disruptions under, 6.23

Arbitration

See also **Alternative Dispute Resolution (ADR)**

Browse-wrap agreement, enforceability of arbitration provision in, 7.4

Domain names. See **Domain Names**

World Intellectual Property Organization (WIPO), model contract clauses requiring submission of disputes to mediation or arbitration by, 21.9

Artists' Rights and Theft Protection Act of 2005 (ART Act), 1.8C

Assignment

See also **Transfer of Property**

Copyright, assignment of. See **Copyrights**

Domain names. See **Domain Names**

Intellectual property, generally, 5.1-5.2, 5.3

Invention assignment. See **Confidentiality and Invention Assignment Agreements**

Patents, assignment of. See **Patents**

Software license, assignment of, 12.12

Trademark, assignment of. See **Trademarks, Service Marks, and Trade Names**

Association or Cooperative

Collective mark used by members of, 3.27

Attorney-Client Privilege

Fed R Evid 502, 20A.44A

Waiver of, 20A.7

Attorney-Client Relationship

Ethical considerations and conflicts of interest in employment negotiations as result of attorney working with company founders and executives, 4.2

Attorneys

Advertising legal services on Internet, effect of ethics rules on, 17.10A-17.10D

Attorney-client privilege. See **Attorney-Client Privilege**

Attorneys general. See **Attorneys General**

Discovery of electronically stored information (ESI), attorney's role. See **Electronically Stored Information (ESI), Discovery of**

Fees. See **Attorneys' Fees**

Loan transactions, legal opinion required for, 16.21

Venture capital financing agreements including opinion of counsel, 16.8

Website development agreements, role of attorney in drafting and negotiating, 5.1, 5.5-5.6

Attorneys' Fees

Anticybersquatting Consumer Protection Act (ACPA), recovery of fees for infringement of domain name, 3.22

Anti-SLAPP statute, recovery of fees under, 20.25

California's anti-spam law, recovery of attorney's fees under, 17.25

Copyright infringement action, recovery of fees in. See **Infringement of Copyright**

Trademark infringement action, recovery of attorney fees in, 3.30, 3.63

Venture capital financing, attorney's fees associated with, 16.8

Attorneys General

California's anti-spam law, right of civil action on part of state attorney general created by, 17.25

CAN-SPAM Act, limited rights of state attorneys general to bring civil suits to enforce, 17.22

At-Will Employment. See Employers and Employees

Audio Home Recording Act of 1992 (AHRA), 8.24, 8.27

Audits

Portal agreements, audit rights provisions, 17.36

Bad Faith

California anti-cybersquatting statute, bad faith requirement under, 20.32

Domain name, factors in determining owner's bad faith use of, 3.13

Bandwidth

Co-location services, size of bandwidth provided under, 6.15

Bankruptcy, Impact on Software License Agreements. See Software License Agreements

Banner Advertising

Cost per thousand (CPM) measurement for banner advertising, 17.31

Form of banner advertising agreement, 17.32

Generic English words or trademarks, effect of using in banner ads, 3.76

Third party website, banner advertisements on, 17.1

BBS. See Bulletin Boards

Beta Testing

Online beta user evaluation agreement, 8.6, 8.7

Better Business Bureau

Privacy seal indicating business' adherence to online Privacy Participation Agreement, 21.19

BidPay (Western Union), 10.6

Blocking Software. See Filtering Software

Board of Directors. See Directors and Officers

Bomb, 18.1

Branding. See Co-Branding

Breach of Contract

Software license, effect of rejecting, 12.12

Bridge Loans, 16.3, 16.7, 16.34

Browse-Wrap Agreements

Defined, 7.1

Enforceability of, 7.4, 8.2

Notice requirements, 7.4

Privacy policy statements, 7.4

Software license modifications, 7.4

Terms of use. See **Terms of Use**

Uniform Computer Transactions Act (UCITA), effect of, 7.11

Bulletin Boards

Copyright infringement, liability of BBS operator for infringing activities of third persons. See **Infringement of Copyright**

Defamation. See **Defamation**

Obscene materials, conviction for interstate transmission of, 20.16

Uploading content to bulletin board systems, 8.19-8.20

Burden of Proof

See also **Evidence; Proof**

Defamation action, 20.2

False or misleading advertising, plaintiff's burden of proving, 17.9

Personal jurisdiction, defendant's burden to show court's unreasonableness in exercising, 19.7

Trade dress, plaintiff's burden of proof in action for infringement of unregistered, 3.77

Trademark infringement action, plaintiff's burden of proof in, 3.60

Trade secret, plaintiff's burden of proof in action for misappropriation of, 2.34

Business Acquisitions. See Acquisitions and Sales of Internet-Based Businesses

CAN-SPAM Act

Generally, 17.11-17.12, 18.4

Affirmative consent, 17.18, 17.20

Attribution rules, 17.21

Deceptive e-mail practices, 17.19

Enforcement, 17.22

Exemptions, 17.13, 17.18

Forwarding commercial e-mails, 17.18A

Identification as advertisement, 17.14-17.15, 17.18, 17.20

National "Do-Not-E-Mail" registry, 17.23

Opt-out requests, 17.12, 17.14, 17.16, 17.18, 17.20

Penalties for violations, 17.20, 17.22, 17.23B

Postal address requirement, 17.14, 17.17, 17.20

Preemption of state law by Act, 17.12, 17.25-17.26

Primary purpose of e-mail under Act, determining, 17.13

Sexually oriented materials, 17.18, 17.20, 17.22

Wireless devices, commercial e-mails sent to, 17.23A

Catalog Sales

Governing law, 17.8, 17.10

Cease and Desist

Complaint site, sending cease and desist letter to, 20.33

Trade or service mark, owner's cease and desist letter to infringer of, 3.69, 3.70

Certificates and Certifications

Contractual certifications, third party's agreement to comply with U.S. export control laws, 21.56

European Union Data Protection Directive, safe harbor certification, 21.12

National Institute of Standards Technology certification of electronic data discovery (EDD) software's ability to forensically extract and examine data, 20A.34

Security certificates, 10.11

Website privacy seal program, certification from nonprofit organization, 9.42

CFAA. See Computer Fraud and Abuse Act (CFAA)

Charts, Checklists, Questionnaires, and Tables

Digital Millennium Copyright Act. See **Digital Millennium Copyright Act (DMCA)**

Due diligence procedures for intellectual property, 22.5, 22.12, 22.13

Open source software, checklist for acquiring, 22.13B

Responding to cyberattack, checklist, 18.23

Checks

Internet checks, 10.5

Child Pornography

See also **Pornography**

Generally, 20.13, 20.17

Child Online Protection Act, provisions of, 20.20

Child Pornography Prevention Act (CPPA), provisions of, 20.19

Children's Internet Protection Act (CIPA), filtering of Internet sites by public schools and libraries, 20.21

Constitutional issues

Child Online Protection Act, constitutionality of, 20.20

Child Pornography Prevention Act (CPPA), unconstitutionality of provisions prohibiting "virtual" child pornography, 20.19

Children's Internet Protection Act (CIPA), constitutionality of, 20.21

Communications Decency Act (CDA), unconstitutionality of provisions relating to transmission of obscene material to minors, 20.5, 20.18

First Amendment considerations affecting libraries' installation of blocking software to prevent minors access to pornographic materials, 20.15

Children

Bullying by electronic act, Ed C §§32261, 32265, and 48900 prohibiting, 20.22A

Child pornography. See **Child Pornography**

Children's Online Privacy Protection Act (COPPA)

Generally, 9.28-9.29

Application of COPPA, 9.30

Enforcement, 9.33

Parental consent, 9.32

Requirements for online collecting of information from children, 9.31

Safe harbor from parental consent requirement, 9.34

Communications Decency Act (CDA), unconstitutionality of provisions relating to transmission of obscene material to minors, 20.5, 20.18

Consent of parents (see Children's Online Privacy Protection Act (COPPA), above)

Data mining by website, FTC enforcement actions to protect young students and children, 9.9

Dot-Kids Act, 9.35

First Amendment considerations affecting libraries' installation of blocking software to prevent minors access to pornographic materials, 20.15

Harmful matter, California Pen C §313 prohibiting distribution to minors, 20.22

Kidz Privacy, 9.36

Choice of Forum Clause

Click-wrap agreement's forum selection clause, enforceability of, 7.3

Distinction between exclusive and nonexclusive choice-of-forum clauses, 19.12

Enforceability of, 19.12

Form, choice of forum clause, 19.13

Fraud, effect on enforceability of choice of forum clause, 19.12

Software license agreements, choice of law or choice of forum provisions, 8.4

Terms of use policy specifying choice of forum and choice of law governing conflicts arising from use of website, network, or systems of company, 8.2

Uniform Computer Transactions Act (UCITA), choice-of-forum provisions in, 7.11

Choice of Law

See also **Conflicts of Law**

Conflicts-of-law principles, exclusion of, 19.21

Drafting considerations, 19.21

Enforceability of choice-of-law clauses

California statutes governing choice-of-law clauses, 19.19

Test for determining, 19.20

Form, choice of law clause, 19.22

Software license agreements, choice of law or choice or forum provisions, 8.4

Terms of use policy specifying choice of forum and choice of law governing conflicts arising from use of website, network, or systems of company, 8.2

Uniform Computer Transactions Act (UCITA), choice-of-law provisions in, 7.11

Click-Free Agreements. See Browse-Wrap Agreements

Click-Wrap Agreements

Generally, 7.3

Defined, 7.1

Enforceability of, 7.3, 7.5, 7.14

E-Sign, effect of, 7.5

Hosting agreements, 6.2

Nonexclusive license, click-wrap agreement as, 12.3

Uniform Computer Transactions Act (UCITA), effect of, 7.11

Co-Branding

Advertising, 17.1

Creation of co-branded page, 11.6

Sample co-branding agreement, 11.7

Coding

See also **Source Code Escrow**

Company access to website source code assisting subsequent developers, 5.26

Cookies, 18.9

Exclusive software licenses used to keep competition from accessing improvements to licensor's base code, 12.2

Open source code, 8.8, 8.9

Proprietary source code, 16.5

Shelf code, use of, 5.15, 5.18-5.19

Warranty in hosting agreement providing that servers and software free from viruses and harmful code, 6.10

Co-Location Agreements

Generally, 6.13

Advantages of, 6.15

Customer responsibilities, 6.16

Equipment considerations, 6.20

Factors in deciding to co-locate, 6.14

Fee for early termination, 6.18

Force majeure clause, 6.18

Form of co-location agreement, 6.18, 6.19

Hosting agreements distinguished, 6.14, 6.20

Negotiability of, 6.18

On-site service plans to repair equipment problems, 6.20

Provider warranties, 6.17

Remote reboot service, 6.16

Services provided by co-location agreement, 6.13, 6.15-6.16

Warranties

Disclaimer of warranties under co-location agreement, 6.18

Provider warranties under co-location agreement, 6.17

Common Law

Conversion, common law tort of, 20.11

Ownership of inventions made on the job by employee, 4.7

Privacy, 9.17

Publicity, common law right of, 20.9

Trademarks, common law protection for unregistered, 3.31

Trade names, common law protection for, 3.27

Communications Decency Act (CDA)

Children, unconstitutionality of provisions restricting transmission of indecent material to, 20.5, 20.18

Defamation actions. See **Defamation**

Compensation

Service level agreement, compensating customer when service falls below agreed level of uptime, 6.24

Term sheet for preferred stock financing, employee compensation provision in, 16.10

Complaints

Domain name infringement, complaint for. See **Domain Names**

Motion to strike complaint under California's Anti-SLAPP statute, 20.25

Complaint Sites

Generally, 20.26

Actions by business owner to prevent operation of complaint sites, 20.33

Cybersquatting, federal and state laws prohibiting

ACPA. See **Anticybersquatting Consumer Protection Act (ACPA)**

Anti-cybersquatting statute (California), 20.32

Uniform Domain Name Dispute Resolution Policy (UDRP), applicability to complaint sites, 20.30

Potential causes of action against complaint site

Generally, 20.27

Cybersquatting (see Cybersquatting, federal and state laws prohibiting, above)

Defamation, 20.28

Trademark infringement and dilution, 3.64, 20.29

Comprehensive General Liability Insurance. See Insurance for On-Line Businesses

Computer Fraud and Abuse Act (CFAA)

See also **Cyberattacks**

Generally, 18.3

Cookies, applicability to, 18.9

Criminal penalties under, 9.14, 18.3, 18.12

Damages, 17.28, 18.7

Definitions

Damage, 18.7

Exceeds authorized access, 18.5

E-mail

Improper use of e-mail, applicability of Act to, 18.7

Spam e-mail, applicability to, 18.3-18.4

Injunctive relief under, 17.28

Physical loss or damage under CFAA, 20.38

Private right of civil action, 9.14

Terms of use, applicability to conduct exceeding, 18.5

Tracking software, applicability to, 18.6

Wireless networks, applicability to, 18.7A

Confidentiality

See also **Disclosure; Privacy**

Acquisitions and sales of Internet-based business, confidentiality agreement on due diligence disclosure, 22.4

Gramm-Leach-Bliley Act, regulation of financial institutions' handling of consumer information, 9.12

Nondisclosure agreements. See **Nondisclosure Agreements**

Source code license instead of source code escrow, confidentiality issues, 15.1

Term sheet for preferred stock financing, confidentiality provision in, 16.10

Trade secrets. See **Trade Secrets**

Website development agreement, confidentiality provisions of, 5.20, 5.26

Confidentiality and Invention Assignment Agreements

See also **Nondisclosure Agreements**

Generally, 4.6, 4.10

Federal work for hire doctrine, 4.8

Independent contractors, 4.18

Sample form, 4.11

Scope of employment, ownership of inventions made within, 4.7

State law, employer ownership of employee inventions, 4.9

Statutory limitations to invention assignment agreements, 4.10

Conflict of Interest

See also **Ethics**

Attorney working with company founders and executive, 4.2

Conflicts of Law

See also **Choice of Law**

Generally, 19.14

Choice-of-law provision, drafting to exclude conflicts-of-law rules of particular jurisdiction, 19.21

Constitutional analysis, 19.15

Governmental interest analysis to resolve conflicts-of-law issues, 19.17

Online businesses' liability based on laws of other states or countries, 19.18

Statutory provision affecting contracts lacking choice-of-law clause, 19.16

Consent

CAN-SPAM Act, affirmative consent under, 17.18, 17.20

Civil penalties or injunction sought by FTC for company's violation of consent order, 17.6

Cookies, consent to interception of electronic communication through use of, 18.9

Electronic discovery, party's consent to production of image file required for, 20A.41

E-Sign, consumer's affirmative consent to receive information in electronic form under, 7.7

FTC's Mail or Telephone Order Merchandise Rule, customer's consent to delay under, 10.16

Parental consent. See **Children**

Uniform Electronic Transactions Act (UETA), consent under, 7.10

Consideration

Software licenses, consideration for, 12.2, 12.5

Constitutional Law

Child pornography. See **Child Pornography**

Conflicts-of-law, constitutional analysis of, 19.15

Copyright protection, basis for, 1.1

Digital Millennium Copyright Act (DMCA), constitutionality of anti-circumvention provisions of, 1.28

First Amendment issues. See **Freedom of Speech in Cyberspace**

Jurisdiction, constitutional limits on. See **Jurisdiction**

Patents, constitutional basis for, 2.2

Privacy. See **Privacy**

Sales and use tax on e-commerce transactions, constitutionality of state imposing, 10.23

Spam e-mail, constitutional issues, 17.11, 20.24

Construction and Interpretation

See also **Definitions**

Browse-wrap agreements, 7.4, 8.2

Clawback of privileged material, 20A.9, 20A.18C, 20A.44

Compensation test for computer programmers, 4.12

Digital Millennium Copyright Act (DMCA), construction of. See **Digital Millennium Copyright Act (DMCA)**

Duties test for computer programmers, 4.12

Initial interest confusion doctrine, 3.73

Lanham Act, 17.3

Libel statute, 20.2

Open-source license, 8.8

Patent infringement action focusing on construction and interpretation of claims in patent application, 2.12

Updates versus new versions of software, 6.42

Website development agreement's ambiguous language construed against drafter, 5.5

Work made for hire doctrine, 5.12

Constructive Notice

Copyright, recordation of transfer document as constructive notice to third parties of transfer, 1.9

Trademark, registration providing constructive notice of ownership, 3.30

Consumer Information. See Privacy

Consumer Protection

Anticybersquatting Consumer Protection Act. See **Anticybersquatting Consumer Protection Act (ACPA)**

E-sign, consumer protection features, 7.7

FTC's Bureau of Consumer Protection, 17.6

Gramm-Leach-Bliley Act, FTC privacy rules for financial institutions' handling of consumer information, 9.12

Content of Website, Obtaining Licenses and Rights to Use

Generally, 14.1, 14.8

Creative commons and other innovative licensing solutions, 14.18

Digital reprint rights license, 14.13, 14.14

Exemption from infringement liability, determination of

Fair use of copyrighted work, 14.6

Public domain, use of work with expired copyright, 14.5

Music licensing, 14.17

Patent infringement, use of unlicensed software as, 14.4

Personal noncommercial use of work, online license restriction, 14.8

Steps to obtaining rights

Generally, 14.1

Exemption from infringement (see Exemption from infringement, determination of, above)

Identifying third-party elements, 14.2

Owners of intellectual property work, identifying, 14.7

Protected exclusive rights of copyright owner, determining, 14.4

Protection of third-party elements by copyright or other intellectual property laws, determination of, 14.3

Still photograph license, 14.11, 14.12

Streaming video license, 14.15, 14.16

Trade secrets, review of website to protect, 14.4

Videotape of testimonial (individual release), sample endorsement agreement, 14.9, 14.10

Contractors. See Independent Contractors

Contracts

Acquisitions and sales of Internet-based businesses. See **Acquisitions and Sales of Internet-Based Businesses**

Advertising agreements. See **Advertising**

Advisory board letter agreement, 4.23

Banner advertising agreement, 17.32

Breach of contract. See **Breach of Contract**

Browse-wrap agreements. See **Browse-Wrap Agreements**

Choice of forum clauses. See **Choice of Forum Clause**

Choice-of-law clauses. See **Choice of Law**

Clip-wrap agreements. See **Click-Wrap Agreements**

Co-branding agreement, 11.7

Co-location agreements. See **Co-Location Agreements**

Confidentiality agreement. See **Confidentiality**

Confidentiality and invention assignment agreement. See **Confidentiality and Invention Assignment Agreements**

Conflicts of law. See **Conflicts of Law**

Credit card processing service, contract with, 10.7

Domain name, purchase of. See **Domain Names**

Electronic contracting. See **Electronic Contracting**

Endorsement agreement, videotape of testimonial (individual release), 14.9, 14.10

European Union Directives. See **European Union Directives**

Executory contracts

Defined, 12.12

Domain name based on executory contract not subject to garnishment, 16.30

Export control laws, third party vendors and customers' agreement to not export or reexport software in violation of, 21.56

Healthcare information disclosures to business entity, HIPPAA contract privacy provisions, 9.11

Hosting agreements. See **Hosting Agreements**

Independent contractors. See **Independent Contractors**

International issues affecting. See **International Issues Affecting E-Businesses**

Invention assignment. See **Confidentiality and Invention Assignment Agreements**

Licenses. See **Licenses**

Nondisclosure agreement. See **Nondisclosure Agreements**

Online beta user evaluation agreement, 8.6, 8.7

Portal agreements, audit rights provisions, 17.36

Privacy Participation Agreement, privacy seal indicating business' adherence to online, 21.19

Protection of Consumers in Respect to Distance Contracts, 21.14

Security agreement, 16.21

Service level agreements. See **Service Level Agreements (SLAs)**

Shrink-wrap license agreements. See **Shrink-Wrap License Agreements**

Software license agreements. See **Software License Agreements**

Source coded escrow agreement, 5.26

Streamlined Sales Tax Agreement, 10.20A

Technical support agreements. See **Technical Support**

Term sheet for preferred stock financing, 16.8-16.9, 16.10

Terms of use policies. See **Terms of Use**

Trademark, licensing agreement for, 3.56

Videotape of testimonial (individual release), sample endorsement agreement, 14.9, 14.10

Warranties. See **Representations and Warranties**

Website development agreements. See **Website Development**

Conversion

Domain name as intangible personal property right protected by conversion law, 20.11

Promissory note, conversion of, 16.35

Term sheet for preferred stock financing, optional conversion rights in, 16.10

Cookies

Blocking cookie files, 9.4

California constitutional claims of violation of privacy, 9.16

Computer Fraud and Abuse Act, applicability of, 18.9

Customer personal information, online businesses obtaining, 9.4

Electronic Communications Privacy Act (ECPA), applicability of, 18.9

Cooperative. See Association or Cooperative

Copyrights

See also **Digital Millennium Copyright Act (DMCA); Infringement of Copyright**

Generally, 1.1

Assignment of copyright (see Transfer of copyright, below)

Contents of website, obtaining rights to. See **Content of Website, Obtaining Licenses and Rights to Use**

Copyright Revision Act of 1976, 1.1

Definitions

Circumvention of technological measure, 1.25

Compilation, 1.2

Contributory infringer, 1.13

Derivative work, 1.6

Direct infringer, 1.13

Joint works, 1.4

Transfer of copyright, 1.9, 16.27

Vicarious infringer, 1.13, 1.16

Work made for hire, 1.5

Derivative works

Defined, 1.6

License to authorize reproduction, distribution, and preparation of, 6.9

Duration of copyright, 1.3

Fair use, factors in determining

Generally, 1.18

Amount of copyrighted work used, 1.21

Contents of website, effect of fair use doctrine on infringement liability, 14.6

Effect of use on potential market or on value of copyrighted work, 1.22

Infringement claim, defense to, 8.27, 14.6

Nature of copyrighted work, 1.20

Published versus unpublished works, 1.20

Purpose and character of use, 1.19

First sale doctrine, 1.23

Hosting customer's website, use of copyrighted content for, 6.9

Independent contractors, online businesses dealing with intellectual property issues, 4.18

Infringement of copyright. See **Infringement of Copyright**

Joint works

Generally, 1.4

Independent contractor as joint owner, 4.18

Music on Internet. See **Music on Internet**

Notice of copyright, benefits of, 1.7

Originality, importance of, 1.2

Ownership of copyrighted works

Generally, 5.1

Distribution rights, 1.6B

First sale doctrine, effect on owner's rights, 1.23

Infringement of owner's rights. See **Infringement of Copyright**

Joint works (see Joint works, above)

Performance rights, 1.6C

Reproduction rights, 1.6A

Rights of copyright owner, generally, 1.6

Work made for hire, 1.5

Photographs, copyright protection for. See **Photographs**

Pre-1978 works, duration of copyright protection for, 1.3

Public domain, works in, 1.3, 14.5

Registration of copyright

Generally, 1.8, 5.1, 16.27

Advantages of registration, 1.8

Distinction between registered and unregistered copyrights, 16.27

Infringement of registered copyright. See **Infringement of Copyright**

Procedures, 1.8A

Time considerations, 1.8B

Security interests in copyrights, perfecting, 16.27

Tangible expression of ideas, copyright protection limited to, 1.2

Third parties

Actual or constructive knowledge by defendant of direct infringement by third parties as requirement for establishing contributory infringement, 1.15

Recordation of transfer document as constructive notice to third parties of transfer of copyright, 1.9

Trade secrets as copyrightable, 16.31

Transfer of copyright

Generally, 1.9, 5.1, 16.27

Form, transfer and assignment of copyright, 1.10

Joint author's assignment not exceeding extent of ownership interest in work, 1.4

U.S. Copyright Office Cover Sheet, 1.11

Types of works protected by copyright law, 1.2

Uniform Computer Transactions Act (UCITA) conflicting with federal copyright law, 7.11

Watermarking technology used to tag visual images and other content, 8.20, 8.22

Work made for hire

Doctrine of, 4.8

Duration of copyright for, 1.3

Ownership of, 1.5

Website's exemption from doctrine of, 5.12

Corporations

Ownership interests, 16.2

Shareholders. See **Shares and Shareholders**

Costs

See also **Fees**

Anti-SLAPP statute, recovery of costs under, 20.25

Banner advertising, cost per thousand (CPM) measurement for, 17.31

Copyright infringement action, recovery of costs in. See **Infringement of Copyright**

Electronic data discovery, costs of, 20A.32, 20A.40, 20A.49

Loan, cost of legal opinion included in estimating transaction costs for, 16.21

Spam e-mail. See **Spam E-Mail**

Trademark infringement action, recovery of costs in, 3.63

Covenant Not to Compete

Trade secrets, California courts' rejection of inevitable disclosure doctrine, 2.26

Covenants

Negative loan covenants, effect of, 16.24

Credit Cards

See also **Debit Cards**

Debt financing, corporate credit cards as method of, 16.17

Online transactions

Contract with credit card processing service, 10.7

Fees, 10.3, 10.7

Processing credit card transactions, 10.3

Secure transaction processing software, 10.3, 10.8

Shopping cart service provided by credit card processor, 10.12-10.13

Criminal Law

Generally, 20.12

Bus & P C §17538 violations, fine or imprisonment for, 17.10

CAN-SPAM Act violations, criminal penalties for, 17.20, 17.22, 17.23B

Child pornography. See **Child Pornography**

Computer Fraud and Abuse Act (CFAA), criminal penalties under, 9.14, 18.3, 18.12

Copyright infringement, criminal liability for, 1.17

Digital Millennium Copyright Act, anti-circumvention provisions of, 18.13

Electronic Communications Privacy Act (ECPA), 9.15, 18.8

Export Administration Regulations (EAR), criminal penalties for violation of, 21.25

Family Entertainment and Copyright Act, investigation and conviction of file swappers for infringing activities under, 8.26B

Forensic images, collection of, 20A.37

Legislation addressing computer crimes, generally, 18.2, 18.14

No Electronic Theft Law (NET Act), criminal prosecution for sound recording infringements under, 8.26

Obscene materials, limitations on criminal statutes regulating, 20.16

Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act), 18.8

Pen C §502 violations, 17.27, 18.16

Pen C §653aa (Internet piracy) prohibiting mass-distribution of video, music, or other files without providing links to source, 8.26A

Stored Communications Act, 18.8, 18.11

Trade secrets, criminal and monetary penalties under Economic Espionage Act of 1996 for misappropriation of, 2.38

USA Patriot Act cyberterrorism provisions, 18.12

Wiretap Act, 18.8

Customer Lists

Trade secret protection for, 2.22-2.23

Customers

Advance payments by customers, businesses seeking, 16.19

Co-location agreements, customer's responsibilities under, 6.16

Hosting agreements

Disclaimer of warranties by customers, 6.10-6.11

Responsibilities of customer under, 6.9

Software access for customers or employees as responsibility of host, 6.4, 6.6

Privacy rights. See **Privacy**

Service level agreements

Generally, 6.33

Compensating customer when service falls below agreed level of uptime, 6.24

Reports by service provider, customer's request for, 6.35

Software access for customers or employees, provisions for, 6.4, 6.23

Technical support. See **Technical Support**

Cyberattacks

See also **Computer Fraud and Abuse Act (CFAA)**; **Viruses**

Generally, 18.1

Bomb, 18.1

Denial of service (DoS) attacks, 18.1

FTC enforcement, online company's failure to protect customer information from known hacker attacks, 9.9A

Pen C §502, penalties for hacking under, 17.27, 18.16

Responding to cyberattack

Generally, 18.22

Checklist, 18.23

Stored Communications Act to prevent hackers from obtaining, modifying or destroying stored electronic communications, 18.8, 18.11

Techniques, generally, 18.1

Trespass to chattels doctrine, applicability to computer hacking, 18.21A

Trojan horse, 18.1

USA Patriot Act, deterrence and prevention of cyberterrorism under, 18.12

US-CERT (Computer Emergency Readiness Team), purpose of, 18.22

Cyberpiracy

Governing law, 3.22, 17.8

Music downloading, 8.22

Cybersquatters

See also **Anticybersquatting Consumer Protection Act (ACPA)**

California anti-cybersquatting statute, 20.32

Defined, 3.1

Domain names. See **Domain Names**

Trademarks, anti-dilution claim against cybersquatters, 3.67

Cyberterrorism

USA Patriot Act, deterrence and prevention of cyberterrorism under, 18.12

Damages

California's anti-spam law, recovery of damages under, 17.25-17.26

CAN-SPAM Act violations, statutory damages for, 17.22

CC §1798.82 violation, damages for, 18.15

Compensatory damages defined, 18.16

Computer Fraud and Abuse Act, damages under, 17.28, 18.7

Copyright infringement, recovery of damages for, 1.17

Destruction of electronic evidence, damages for, 20A.28

Digital Millennium Copyright Act, recovery of damages under. See **Digital Millennium Copyright Act (DMCA)**

Domain name, recovery of damages for infringement of. See **Domain Names**

False or deceptive advertising, civil lawsuits for refunds to consumers of actual damages relating to, 17.6

No Electronic Theft Law (NET Act) violations, civil liability for damages for, 8.26

Phishing violations, damages for, 3.63, 9.6C

Software license agreements. See **Software License Agreements**

Trademarks. See **Trademarks, Service Marks, and Trade Names**

Trade secret misappropriation, recovery of damages for, 2.36

Treble damages

Patent infringement, recovery of treble damages for, 2.2

Trademark, recovery of treble damages for violating rights of, 3.30

USA Patriot Act, damages for cyberterrorism under, 18.12

Data Custodians. See Electronically Stored Information (ESI), Discovery of

Data Mining. See Privacy

Data Protection Directive. See European Union Directives

Debit Cards

See also **Credit Cards**

Online versus offline debit transactions, 10.4

Debt Financing

See also **Equity Financing**

Generally, 16.11

Agreement for loan, 16.23, 16.24

Angel investors, 16.3, 16.34

Bridge loan from investor, 16.3, 16.7, 16.34

Commercial loans, 16.3

Convertible debt, generally, 16.18

Corporate credit cards, 16.17

Customer advances, 16.19

Elements of simple loan transaction

Generally, 16.21

Usury issues for non-bank lenders, 16.22

Equity financing, debt financing as alternative to, 16.3

Lease financings, advantages of, 16.16

Promissory notes. See **Promissory Notes**

Qualification criteria for loans, 16.20

SBA loans, 16.15

Security interests in intellectual property collateral, perfecting

Generally, 16.3, 16.26

Copyrights, 16.27

Domain names, 16.30

Form of security agreement, 16.32, 16.33

Patents, 16.28

Trademarks, 16.29

Trade secrets, 16.31

UCC-1 financing statement, filing, 16.21, 16.26-16.31

Term loans, 16.14, 16.24

Types of debt financing, generally, 16.12

Working capital loans, 16.13

Declarations. See Affidavits and Declarations

Decompilation

Software license agreements, prohibition on decompilation under, 8.4

Decrees. See Judgments and Decrees

Deeds of Trust, 16.21

Defamation

Generally, 20.1-20.2

Anonymous communications, speaker's liability for defamation, 20.24

Burden of proof in defamation action, 20.2

Communications Decency Act (CDA), effect of (see Subscribers, ISP liability for defamation by, below)

Complaint site, defamation action against, 20.28

Comprehensive general liability insurance, coverage for defamation claims under, 20.35

Cyberspeech as libel or slander, 20.3

Defenses of ISP to defamation (see Subscribers, ISP liability for defamation by, below)

First Amendment protection for defamation, lack of, 20.15

Identities of persons making defamatory statements, ISP's disclosure of, 20.3

Immunity of ISP (see Subscribers, ISP liability for defamation by, below)

Opinions, qualified privilege for, 20.3, 20.15

Subscribers, ISP liability for defamation by

Distributor or publisher, characterizing ISP as, 20.4

Foreign law, lack of immunity under, 21.3

Good Samaritan exemption under Communications Decency Act (CDA), 20.5, 20.28

Preemption of state law under Communications Decency Act (CDA), 20.7

Scope of immunity under Communications Decency Act (CDA), 20.6-20.6D

Vicarious liability for subscribers' defamatory statements, ISP's immunity under Communications Decency Act (CDA) from, 20.1, 20.5, 20.28

Default and Default Judgments

Hosting agreement terminated in event of default by host, 6.10

Multiple loan obligations to single creditor, cross-default provisions imposed by lender when, 16.24

Sanction for willfully thwarting discovery, entry of default judgment against offending party as, 20A.28

Secured debt, effect of company defaulting on, 16.3, 16.21

Defenses

Child Pornography Prevention Act (CPPA), affirmative defenses under, 20.19

Communications Decency Act (CDA), ISP's defenses against defamation claim under. See **Defamation**

Fair use doctrine. See **Copyrights**

Immunity. See **Immunity**

Right of publicity, defenses in action for commercial misappropriation, 20.9

Statute of limitations. See **Statutes of Limitations**

Trademarks. See **Trademarks, Service Marks, and Trade Names**

Trade secrets, defenses to claim of misappropriation, 2.35

Definitions

See also **Construction and Interpretation**

Advertainment, 17.30

Advertisement, 20.41

Adware, 9.6A

Affirmative consent, 17.18

Aggregators, 8.17

Ancillary cryptography, 21.34A

Angel investors, 16.6

Arbitrary or fanciful mark, 3.28

Assignments in gross, 3.57

Blurring of mark, 3.65

Bomb, 18.1

Bots, 8.17

Bridge loan, 16.3

Browse-wrap or click-free agreement, 7.1

Burning (CDs), 8.22

Business associate, 9.11

Business method, 2.18

Canned software, 10.25

Certification mark, 3.27

Child pornography, 20.19

Click-through percentages, 17.31

Click-throughs, 8.18

Click-wrap agreement, 7.1

Cloaking, 17.29B

CODEC, 8.22

Coined mark, 3.28

Collective mark, 3.27

Comity, 21.5

Commercial advantage or private financial gain (NET Act), 8.26

Commercial electronic mail messages, 17.13

Commercial general liability insurance, 20.35

Commercial name, 3.27

Computer Fraud and Abuse Act. See **Computer Fraud and Abuse Act (CFAA)**

Convertible debt, 16.18

Cookies, 9.4, 18.9

Copyright management information (CMI), 1.25A

Copyrights. See **Copyrights**

Covered property, 20.36

Crawlers, 7.4, 8.17

Cryptanalytic items, 21.44

Custom software, 10.25

Cybersquatters, 3.1

Deep linking, 8.15

Denial of service (DoS) attacks, 18.1

Descriptive mark, 3.28

Design patent, 2.3

Dictionary attacks, 17.19

Digital audio recording devices, 8.24

Digital signature, 7.6

Dilution of mark, 3.65

Distributed denial of service (DDoS) attacks, 18.1

Domain name, 3.1, 16.30

Domain name change in ownership, 22.18

Domain Name System (DNS), 3.1

Domain name transfer or assignment, 22.18

Downloading, 8.19, 8.22

Electronically stored information (ESI), discovery of. See **Electronically Stored Information (ESI), Discovery of**

Electronic Communications Privacy Act. See **Electronic Communications Privacy Act (ECPA)**

Electronic data, 20.41

Electronic signature, 7.5

Electronic storage, 18.11

Executory contract, 12.12

Exit strategy, 16.4

Export, 21.24

Famous mark, 3.66

File Transfer Protocol (FTP), 8.19

Firewalls, 2.27

First party coverage, 20.35

Foreign national, 21.24

Framing, 8.15

Functionality (of design or appearance), 3.80

Functional specification, 5.16

Generic mark, 3.28

Googlebowling, 17.29B

Harmful matter, 20.22

Harvesting, 17.19

Hypertext reference, 8.15

Image link, 8.15

Impressions, 17.31

Information content provider, 20.5

Inline link, 8.15

In rem jurisdiction, 19.11

Intellectual property, 16.26

Intercept, 18.11A

Internet Protocol, 3.1

Internet service provider, 1.30

IP address, 3.1

Item, 21.23

Joint works, 1.4

Jurisdiction, 19.1

Keying, 3.73

Knowledge, 21.50

Libel, 20.2

Limited cryptography, 21.34

Link, 8.15

Mark, 3.26

Mass market item (encrypted software), 21.33

Metadata, 12.6

Mousetrapping, 17.7

MP3, 8.22

Naked trademark license, 3.53

Object code, 15.1, 21.30

Offline debit cards, 10.4

Open relay, 17.29

Operation technology, 21.48

Out link, 8.15

Palming off, 3.61

Patent, 2.1-2.2

Patent prosecution, 2.10

Peer-to-peer (P2P) files, 8.27

Penal Code §502

Compensatory damages, 18.16

Computer contaminant, 18.16

Injury, 18.16

Person, 17.9

Personal information, 9.25, 9.31, 18.15

Personal jurisdiction, 19.1

Phishing, 9.6C

Physical damage, 20.36, 20.38

Plant patent, 2.3

Principal register, 3.28

Prior art, 2.8

Privacy seal program, 9.43

Protected computers (USA Patriot Act), 18.12

Publicly available software, 21.29

Reexport, 21.51

Registrar, 3.6

Reverse engineering, 2.24

Reverse palming off, 3.61

Ripping, 8.22

Robot, 7.4

Royalty base, 12.5

Search engine optimization (SEO), 17.29A

Secondary domain names, 3.2, 20.33

Secondary meaning (of trademark), 3.34

Secure transaction processing software, 10.8

Security certificates, 10.11

Service, 3.27

Service level agreement (SLA), 6.1, 6.21

Service mark, 3.27

Service provider, 1.30

Service provider under Gramm-Leach-Bliley Act, 9.12

Shelf code, 5.15

Shopping carts, 10.12

Shop right, 4.7

Shrink-wrap license agreement, 7.1

Signed (UCC), 7.5

Slander, 20.2

Software license, 12.1

Source code, 15.1, 21.30

Source code escrow, 15.1

Spam, 17.1, 20.24

Spiders, 7.4

Spoofing, 17.19, 17.28

Spyware, 9.6B

Strategic alliance, 11.1

Strategic partners, 16.7

Streaming audio, 8.22

Suffix, 3.3

Suggestive mark, 3.28

Sweat equity, 16.5

Tangible, 20.36

Targeted to children, 9.30

Tarnishment of mark, 3.65

Technical data, 21.48

Technology, 21.48

Term loans, 16.14

Term of patent, 2.4

Terms of use, 8.1

Third party coverage, 20.35

Tracking software, 9.6

Trade dress, 3.27, 3.77

Trademark, 3.27

Trade name, 3.27

Trade secret, 2.21, 2.38, 4.6

Transactional or relationship (e-mail) message, 17.13

Trojan horse, 18.1

Trustmark, 21.19

Typo-squatters, 3.2

Unfair competition, 9.27

Uniform Resource Locator (URL), 3.1

Unregistrable mark, 3.32

Uploading, 8.19

URL, 3.1

Use of trademark, 3.53

U.S. subsidiary, 21.39

Utility patent, 2.3

Virus, 18.1

Warrants, 16.2

War spamming, 18.7A

Web bugs, 9.5

Working capital loans, 16.13

Work in public domain, 14.5

Worm, 18.1

Denial of Service (DoS) Attacks, 18.1

Derivative Works. See Copyrights

Design Patents. See Patents

Destruction of Property

Copyright infringement, destruction of infringing articles as remedy for, 1.17

Digital Millennium Copyright Act (DMCA)

See also **Copyrights**

Generally, 1.24

Anti-circumvention of technological protection measures

Generally, 18.13

Anti-circumvention prohibitions, 1.25

Constitutionality of provisions, 1.28

Copyright management information (CMI), protecting integrity of, 1.25A

Exceptions to anti-circumvention prohibitions, 1.26

Remedies for violation of statute, 1.27

Checklists

Compliance with DMCA, checklist for attorneys representing ISPs, 1.43

Notice and take down of infringing material, 1.39

Construction and interpretation of Act

Legislative history of DMCA, courts referring to, 1.42

Safe harbors for ISPs, independent construction of, 1.29

Strict construction of exceptions to anti-circumvention provisions, 1.26

Damages, recovery of

Anti-circumvention prohibitions, recovery of damages for violations of, 1.27

Misrepresentations in notification of infringement, civil damage penalties for, 1.37

Immunity of ISPs (see Information on systems or networks at direction of users, safe harbor for, below)

Impact of DMCA on service providers, 1.42

Information on systems or networks at direction of users, safe harbor for

Generally, 1.33

Agent to receive notification of copyright infringement, ISP designating, 1.34

Checklist for notice and take down of infringing material, 1.39

Claimed infringement, notifying ISPs of, 1.37

Counter-notification by subscriber to have material restored, 1.38

Fraudulent infringement claims, safeguards against, 1.37

Information location tools safe harbor, 1.40

Removal or disabling access to infringing material, 1.36

Right and ability of ISP to control infringing activity, effect of, 1.35

Internet service providers (ISPs), safe harbors limiting liability for infringement

Generally, 1.29

Enforcement of safe harbors, 1.42

General conditions for safe harbors, 1.30

Information residing on systems at direction of user (see Information on systems or networks at direction of users, safe harbor for, above)

System caching safe harbor, 1.32

Transitory digital network communications safe harbor, 1.31

Interpretation of Act (see Construction and interpretation of Act, above)

Notice of copyright infringement (see Information on systems or networks at direction of users, safe harbor for, above)

Purpose of, 1.24

Safe harbors (see Internet service providers (ISPs), safe harbors limiting liability for infringement, above)

Statutory license provisions under DMCA, amendment of, 8.25

Subpoenaing ISPs for names of alleged infringers, 1.29, 1.41

Website's terms of use policy, requirements, 8.2

Digital Performance Right in Sound Recordings Act of 1995 (DPRA), 8.25, 8.27

Dilution of Famous Trademark. See Trademarks, Service Marks, and Trade Names

Directors and Officers

Term sheet for preferred stock financing, board size and composition provisions in, 16.10

Disclaimer of Warranty. See Representations and Warranties

Disclosure

See also **Confidentiality; Privacy**

Data collection and website privacy policies. See **Privacy**

Defamatory statements, disclosure by ISP of persons making, 20.3

Electronically stored information (ESI), initial voluntary disclosure of, 20A.8

FTC's dot com disclosure guidelines, 17.5

Maintenance requirements in service level agreement, disclosure of, 6.25

Nondisclosure agreement. See **Nondisclosure Agreements**

Patent application, required disclosures in, 2.11

Subpoenas. See **Subpoenas**

Trade secrets. See **Trade Secrets**

Vendors taking orders over Internet, disclosure requirements for, 17.10

Website development, disclosure of confidential information associated with, 5.20

Discovery

Electronically stored information (ESI), discovery of. See **Electronically Stored Information (ESI), Discovery of**

Trade secret discovery by reverse engineering, 2.24

Dismissal of Action

Choice-of-forum clause, dismissal for commencing action in forum other than one specified in, 19.12

Destruction of electronic evidence, dismissal for, 20A.28

Domain Names

Generally, 3.1

Anticybersquatting Consumer Protection Act (ACPA)

Generally, 3.22

Attorney fees, recovery of, 3.22

Claim against infringing domain name under, 3.11

Complaint site, applicability of ACPA to, 20.31

Damages, recovery of, 3.22-3.24

Elements of cause of action, 3.23

Enactment of, 3.1, 3.22

Injunction against infringement, 3.24

In rem jurisdiction over domain name, ACPA providing for, 19.11

Remedies available under, 3.24

Uniform Domain Name Dispute Resolution Policy (UDRP) distinguished from, 3.25

Arbitration

Trademarks and domain names, arbitration procedure to resolve infringement claims involving, 20.30

UDRP, arbitration under (see Uniform Domain Name Dispute Resolution Policy (UDRP), below)

Assignment of domain names (see Transferring ownership of domain names, below)

Complaint for infringement (see Uniform Domain Name Dispute Resolution Policy (UDRP), below)

Complaint site

Anticybersquatting Consumer Protection Act (ACPA), applicability to complaint site, 20.31

Purchase of complaint site from operator, 20.33

Registering domain name for, 20.26

Trademark, complaint site's domain name infringing on, 3.64, 20.29

Uniform Domain Name Dispute Resolution Policy (UDRP), applicability to complaint sites, 20.30

Conversion law, domain name as intangible personal property right protected by, 20.11

Cybersquatters

Anticybersquatting Consumer Protection Act (ACPA), registration of intentional misspelling of distinctive domain name as violation of, 3.22

Defined, 3.1

Secondary domain names, registration to prevent registration by cybersquatters, 3.2, 20.33

Trademark registration, benefits of, 3.30

Damages

Anticybersquatting Consumer Protection Act (ACPA), recovery of damages under, 3.22-3.24

Uniform Domain Name Dispute Resolution Policy (UDRP), unavailability of damages under, 3.16

Definitions

Country codes, 3.3

Cybersquatters, 3.1

Domain name, 3.1

Domain Name System (DNS), 3.1

Internet Protocol, 3.1

IP address, 3.1

Registrar, 3.6

Secondary domain names, 3.2, 20.33

Sponsored and unsponsored TLDs, 3.3

Suffix, 3.3

Top-level domain names (TLDs), 3.3

Typo-squatters, 3.2

Uniform Resource Locator (URL), 3.1

URL, 3.1

Due diligence before registration to prevent infringement on third party's trademark

Generally, 3.4

Registered and unregistered trademark searches, 3.5

Infringing domain names

Anticybersquatting Consumer Protection Act (see Anticybersquatting Consumer Protection Act (ACPA), above)

Claim against infringing domain name, 3.11

Commerce, requirement that infringing domain name be used in, 3.67

Due diligence to prevent infringement (see Due diligence before registration to prevent infringement on third party's trademark, above)

Federal and state cyberpiracy statutes, 3.22

Federal Trademark Dilution Act of 1995, trademark owners asserting claims against domain name infringers under, 3.22

Purchase of previously registered domain name infringing on third party's trademark, effect of, 3.7

Trademarks (see Trademarks, below)

Uniform Domain Name Dispute Resolution Policy (see Uniform Domain Name Dispute Resolution Policy (UDRP), below)

Issuance of, 16.30

Loss of domain name, actions causing, 3.9

Purchase of registered domain name

Generally, 3.7

Agreement for purchase of domain name, 3.8

Complaint site, purchasing from operator, 20.33

Owner of famous mark, purchase of domain name for purposes of selling to, 3.67

Registration of domain name

Generally, 3.6, 5.13

Cybersquatters (see Cybersquatters, above)

Due diligence after registration to prevent loss of domain name, 3.9

Due diligence before registration of domain name (see Due diligence before registration to prevent infringement on third party's trademark, above)

Marketing efforts, registration of domain name as part of, 3.1

Purchase of registered domain name (see Purchase of registered domain name, above)

Secondary domain names, registration of, 3.2, 20.33

Registration of domain names as trademarks

Generally, 3.45

Benefits of registration, 3.30

Refusal of registration, grounds for, 3.46

Suffix, registration as trademark, 3.45

Security interests in domain names, perfecting, 16.30

Selection of domain name

Generally, 3.2

Suffix, restrictions on selection of, 3.3

Suffix (top level domain name)

Selection of, 3.3

Trademark, registration of suffix as, 3.45

Third parties, preventing infringement against (see Infringing domain names, above)

Trademarks

Arbitration procedure to resolve infringement claims involving domain names and trademarks, 20.30

Complaint site's domain name infringing on trademark, 3.64, 20.29

Due diligence (see Due diligence before registration to prevent infringement on third party's trademark, above)

Lanham Act, domain name qualifying as trademark under, 16.30

Owner of famous mark, purchase of domain name for purposes of selling to, 3.67

Registration of domain names as trademarks (see Registration of domain names as trademarks, above)

Transferring ownership of domain names

Generally, 3.10, 22.18

Anticybersquatting Consumer Protection Act (ACPA), transferring registration of infringing domain name to trademark holder as remedy under, 3.24

Changing ownership on sale of Internet-based businesses, domain name assignment agreement, 22.18, 22.19

Purchase of domain name (see Purchase of registered domain name, above)

Uniform Domain Name Dispute Resolution Policy (UDRP), transferring registration of infringing domain name as remedy under, 3.16, 3.25

Trespass to chattels claims, 18.19

Truth in Domain Names Act, effect of, 3.2

Uniform Domain Name Dispute Resolution Policy (UDRP)

Generally, 3.11-3.12

Anticybersquatting Consumer Protection Act (ACPA) distinguished from, 3.25

Appeal of arbitration panel's decision, 3.21

Binding arbitration proceeding to resolve infringement claim, 3.12

Complaint sites, application of UDRP to, 20.30

Damages award prohibited under, 3.16

Elements of UDRP claim, 3.13

Fees for arbitration, 3.16

Filing complaint with arbitration provider, effect of, 3.15

Model form of UDRP complaint, 3.17, 3.18

Model form of UDRP response, 3.19, 3.20

Procedures under UDRP, 3.15

Remedies available, 3.16, 3.25, 20.30

Selection of arbitrators, 3.14

WIPO. See **World Intellectual Property Organization (WIPO)**

World Intellectual Property Organization (WIPO), alternative dispute resolution services offered by, 21.9

Downloading and Uploading Content

Generally, 8.19

Bulletin board sites (BBS), 8.19-8.20

Copyright infringement issues, 8.20

File Transfer Protocol (FTP), 8.19

Hosting agreement governing content uploading and maintenance, 6.7, 6.9

Music on Internet, 8.22

Software download and distribution, license agreements governing. See **Software License Agreements**

Terms of use policies on upload of viruses, 8.3

Due Diligence Procedures for Intellectual Property. See Acquisitions and Sales of Internet-Based Businesses

E-Commerce Transactions and Payments

Generally, 10.1

BidPay (Western Union), 10.6

Credit cards. See **Credit Cards**

Debit cards, 10.4

Digital cash, 10.6

Electronic contracting. See **Electronic Contracting**

Fraud prevention tools, 10.8-10.9

General technology companies, e-commerce services provided by, 5.10

Installment payments. See **Installment Payments**

Internet checks, 10.5

Online escrow services, 10.6

PayPal, 10.6

Secure transaction processing software, 10.3, 10.8

Security certificates, 10.11

Shopping cart programs. See **Shopping Cart Programs**

Taxation. See **Tax on Internet Transactions**

Telephone sales. See **Telephone Sales**

Website development

Payments tied to deliverables, 5.16

Specialists, e-commerce services provided by, 5.9

Website end user payment terms, 10.14, 10.15

Economic Espionage Act of 1996

Trade secrets, criminal and monetary penalties for misappropriation of, 2.38

Electronically Stored Information (ESI), Discovery of

Generally, 20A.1

Attorney's role

Identifying data for discovery (see Identifying data for discovery, below)

Legal hold letter to client, sending, 20A.23, 20A.24

Litigation hold letter to opponent, 20A.25, 20A.26

Negotiating ESI discovery plan, 20A.10

Collecting data

Defensible collection strategies, 20A.31

Forensic data professionals, 20A.33

Forensic or mirror images, 20A.37

Metadata, 20A.33, 20A.35-20A.36

On-site inspection, right to, 20A.30, 20A.38

Paper-based versus electronic production, 20A.32

Risk in ESI collection, 20A.35

Software for electronic data discovery (EDD), 20A.32, 20A.34

Costs of, 20A.32, 20A.40, 20A.49

Data custodians

Interviewing, 20A.29

Pending or underway litigation, custodian of discoverable electronic information's obligation to interfere with routine system deletion operations when, 20A.15

Data processing, storage, and review

De-duplication of data, 20A.45

Hosting, 20A.47

Litigation support platforms, 20A.46

Security of data, 20A.48

Definitions

De-duplicated, 20A.45

Electronically stored information, 20A.16

Forensic (or mirror) image, 20A.37

Forensic data collection, 20A.34

Full disk image, 20A.34

Ghost image, 20A.37

Harvested (data), 20A.45

Horizontal de-duplication, 20A.45

Host (data), 20A.47

Image files, 20A.41

Legacy data, 20A.11

Legacy systems, 20A.40

Litigation hold, 20A.21

Litigation hold letter, 20A.25

Logical evidence file (.lef) format, 20A.45

MD5 Hash value, 20A.40

Metadata, 20A.36

Multi-threading, 20A.34

Native (format), 20A.14, 20A.40

Near de-duplication, 20A.45

Platform, 20A.40

Preservation-of-evidence letter, 20A.25

Records, 20A.24

Slack space, 20A.37

Spoliation letter, 20A.25

Spoliation of evidence, 20A.22

Vertical de-duplication, 20A.45

Depositions of IT personnel, 20A.30

Document retention policies, 20A.4

Electronic Discovery Act. See **Electronic Discovery Act**

E-mail, special problems concerning, 20A.5

Federal Rules

Generally, 20A.6

Electronic Discovery Act compared. See **Electronic Discovery Act**

General discovery provisions (Rule 26) (see General discovery provisions (Rule 26), below)

Interrogatory responses (Rule 33), 20A.12, 20A.30

Production of documents and things (Rule 34) (see Production of documents and things, below)

Safe harbor from sanctions for routine deletion (Rule 37), 20A.15

Scheduling orders (Rule 16), 20A.7

Subpoenas, response to (Rule 45), 20A.16

Fed R Evid 502, effect of, 20A.44A

Form of production

Generally, 20A.39

Image files, production of (see Image files, production of, below)

Native format, production in, 20A.40

General discovery provisions (Rule 26)

Clawback of privileged material, 20A.9, 20A.44

Initial voluntary disclosure, 20A.8

Meet-and-confer requirements, 20A.10

Safe harbor limiting potential scope of discovery if ESI not reasonably accessible, 20A.11

Governing law, 20A.17

Hash code technology, use of, 20A.40, 20A.45

Identifying data for discovery

Infrastructure of ESI, need to understand, 20A.29

Request for production, drafting, 20A.30

Image files, production of

Generally, 20A.41

Copying electronic files, 20A.42

Metadata, handling, 20A.43

.tiff images, 20A.41, 20A.46

Initial voluntary disclosure, 20A.8

Interrogatory responses, 20A.12, 20A.30

Legal hold letter to client, 20A.23, 20A.24

Litigation hold

Defined, 20A.21

Litigation hold letter to opponent, 20A.25, 20A.26

Routine deletion operations, no safe harbor for destruction of information subject to litigation hold, 20A.15

Meet-and-confer requirements, 20A.10

Metadata

Collecting data, 20A.33, 20A.35-20A.36

Format changed to eliminate or alter metadata, 20A.14, 20A.33, 20A.40

Handling metadata, generally, 20A.43

Penalties

Conversion of electronic evidence to inaccessible format, sanction for, 20A.27

Failure to comply with federal rules, penalties for, 20A.6

Safe harbor from sanctions for routine deletion (Rule 37), 20A.15

Spoliation of evidence, sanctions for, 20A.19, 20A.22, 20A.28, 20A.33, 20A.35

Pending litigation

Custodian of discoverable electronic information's obligation to interfere with routine system deletion operations when litigation pending or underway, 20A.15

Events constituting indicators of potential litigation, 20A.21

Notice of litigation triggering duty to preserve data, 20A.21-20A.22

Preparation for ESI discovery

Identifying key personnel, 20A.20

Survey and retention policy, 20A.19

Privileged material

Clawback of privileged material, 20A.9, 20A.18C, 20A.44

E-mails, privileged information header or footer added to, 20A.5

Waiver of privilege, 20A.7

Production of documents and things

Generally, 20A.19

Drafting request for production, 20A.30

Form of production (see Form of production, above)

Image files, production of (see Image files, production of, above)

Inspection, copying, testing, and sampling (Rule 34(a)), 20A.13

Specifying format for production (Rule 34(b)), 20A.14, 20A.40

Retention of ESI

Absence of statute or regulation, effect of, 20A.3

Document retention policies, 20A.4

Manner of preservation, 20A.27

Regulatory obligations, 20A.2

Survey and retention policy, 20A.19

Review of data (see Data processing, storage, and review, above)

Safe harbors, 20A.11, 20A.15

Storage of data (see Data processing, storage, and review, above)

Subpoenas, Response to subpoenas (Rule 45), 20A.16

Third-party data-hosting service, use of, 20A.47

Electronic Communications Privacy Act (ECPA)

Generally, 9.15, 18.8

Cookies, applicability to, 18.9

Definitions

Cookie, 18.9

Intercept, 18.8

Elements of claim under ECPA, 18.8

Penalties for privacy violations, 9.15, 18.8

Stored Communications Act (Title II of ECPA), 18.8, 18.11

Tracking software, applicability to, 18.6, 18.10

Unauthorized wireless access, applicability of Act to, 18.11A

Wiretap Act (Title I of ECPA), applicability to intercepted electronic transmissions, 9.15, 18.8

Electronic Contracting

Generally, 7.1, 10.2

Browse-wrap agreements. See **Browse-Wrap Agreements**

Click-wrap agreements. See **Click-Wrap Agreements**

Drafting enforceable electronic agreements, 7.14

Electronic Signatures in Global and National Commerce Act (E-Sign). See **E-Sign**

International issues. See **International Issues Affecting E-Businesses**

Linking agreement, 8.18

Software license agreements. See **Software License Agreements**

Terms of use policies. See **Terms of Use**

Uniform Computer Transactions Act (UCITA). See **Uniform Computer Transactions Act (UCITA)**

Uniform Electronic Transactions Act (UETA). See **Uniform Electronic Transactions Act (UETA)**

Electronic Discovery Act

See also **Electronically Stored Information (ESI), Discovery of**

Generally, 20A.18

Clawback of privileged information, 20A.18C

Court-imposed limits on ESI production, 20A.18E

ESI from sources not reasonably accessible, 20A.18A

Form of ESI production, 20A.18D

Safe harbor provision for lost information, 20A.18B

Electronic Signatures in Global and National Commerce Act (E-Sign). See E-Sign

E-Mail

Advertising. See **Advertising**

Archives containing e-mail messages, availability of copyright protections for, 1.37

CAN-SPAM Act. See **CAN-SPAM Act**

Computer Fraud and Abuse Act. See **Computer Fraud and Abuse Act (CFAA)**

Document retention policies, special problems concerning e-mail under, 20A.5

E-Sign, effect of, 7.6

Export, e-mail qualifying as, 21.24

National "Do-Not-E-Mail" registry, 17.23

Privileged information header or footer added to e-mails, 20A.5

Searches by employer, 9.15

Spam. See **Spam E-Mail**

Specific personal jurisdiction based on e-mails to forum state, 19.9

Terms of use policy, 8.3

Unsolicited e-mail. See **Spam E-Mail**

Wireless devices, commercial e-mails sent to, 17.23A

Employers and Employees

Attorney working with company founders and executives, ethical considerations and conflicts of interest in employment negotiations, 4.2

At-will employment

Generally, 4.3

Offer letter to prospective employee, 4.4, 4.5

Co-location provider's staff, services provided by, 6.15-6.16

Confidentiality and invention assignment agreements. See **Confidentiality and Invention Assignment Agreements**

E-mail

Expectation of privacy by employees using e-mail, limits on, 20A.5

Searches by employer, 9.15

Factors characterizing employer-employee relationship, 1.5

Independent contractors. See **Independent Contractors**

Intellectual property created by employees providing value inherent in business's website, 5.1

Overtime, special rules for computer programmers, 4.12

Overview, 4.1

Public policy favoring employee mobility, 2.26

Senior executives, 4.1

Technical support provided by vendor, 6.43-6.44

Term sheet for preferred stock financing, employee compensation provision in, 16.10

Trademarks, policies prescribing employees' allowable uses of, 3.53

Trade secrets, stressing importance to departing employees, 2.26

Types of employment agreements, 4.1

Venture capital financing agreements including management employment agreements, 16.8

Work made for hire. See **Work Made for Hire**

Encryption Software

Copyright infringement by users, encryption software used to shield service provider from knowledge of, 8.27

Credit card transactions, 10.3, 10.8

Digital Millennium Copyright Act (DMCA), exceptions to anti-circumvention provisions for encryption research, 1.26

Export controls. See **Export Controls on Commercial Software and Technology**

FTC enforcement, online company's failure to protect customer information by encryption from known hacker attacks, 9.9A

Internet checks, 10.5

Other states' data protection programs, 9.27A

Shopping cart services, security and encryption capabilities of, 10.13

Trade secrets, encryption of information transmitted on Internet to prevent access to, 2.27

Endorsement Agreement

Videotape of testimonial (individual release), sample endorsement agreement, 14.9, 14.10

End-User License Agreements (EULAs). See Software License Agreements

Equity Financing

See also **Debt Financing**

Generally, 16.1-16.2

Angel investors, 16.6, 16.34

Cash, 16.5

Common stock, 16.2, 16.5

Debt financing as alternative, 16.3

Exit strategies, 16.4

Founders, friends, and family, 16.5, 16.34

Preferred stock, 16.2, 16.7-16.8

Sources of equity funding, generally, 16.4

Sweat equity, 16.5

Venture capital financing. See **Venture Capital Financing**

E-Sign

Generally, 7.5

Consumer protection features, 7.7

Definitions, 7.5-7.6

Elements required for electronic signature, 7.6

Enforceability of electronic record, 7.8

Retention of electronic records, 7.7-7.8

Uniform Electronic Transactions Act (UETA)

Distinguishing from E-Sign, 7.10

Preemption by E-Sign, 7.9

Ethics

See also **Conflict of Interest**

Attorney working with company founders and executives, ethical considerations in employment negotiations, 4.2

Website development agreement, ethical considerations in drafting, 5.5

EULAs. See End-User License Agreements (EULAs)

European Union Directives

See also **International Issues Affecting E-Businesses**

Generally, 21.10

Data Protection Directive

Generally, 21.11

Case-by-case compliance, 21.13

Compliance with, 21.12-21.13

Model contract clauses to safeguard transfers of data from EU member states to foreign countries, 21.13

Safe harbor certification, company's compliance with seven data protection principles, 21.12

Data retention directive, 21.18A

E-commerce directive, 21.15

Electronic contracting, enforceability of, 7.13

Privacy directive

Generally, 21.18

Safe Harbor Accord, 9.38

Scope of, 9.37

Proof of conformity with minimum safety requirements, requirement of manufacturers providing, 21.17

Protection of Consumers in Respect to Distance Contracts, 21.14

Specific industry directives, 21.17

Value Added Taxes (VAT), EU requiring non-EU vendors of digital products to charge on Internet sales to EU consumers, 21.16

Evidence

See also **Burden of Proof; Proof**

Employee confidentiality agreement, execution as evidence of trade secret protection, 4.6

E-Sign, retention and evidentiary use of electronic records under, 7.7-7.8

Spoliation of evidence

Defined, 20A.22

Sanctions for spoliation of electronic evidence, 20A.19, 20A.22, 20A.28, 20A.33, 20A.35

Spoliation letter to opponent, 20A.25

Trademarks

Abandonment, nonuse of trademark for 3 consecutive years as prima facie evidence of, 3.53

Assignment, notarial acknowledgment as prima facie evidence of, 3.57

Registration as prima facie evidence of validity, 3.30

Uniform Electronic Transactions Act (UETA), retention and evidentiary use of electronic contracts under, 7.9

Executory Contracts. See Contracts

Exemplary Damages. See Punitive Damages

Exhibits

Functional specification as exhibit included with website development agreement, 5.16

Hosting agreements. See **Hosting Agreements**

Royalty report attached as exhibit to software license agreement, 12.7

Source code escrow agreement attached as exhibit to software license agreement, 12.7

Experts and Expert Witnesses

Electronic data collection

Forensic data collection expert, advantages of using, 20A.33

Testimony of expert, methods supported by, 20A.31

Export Controls on Commercial Software and Technology

Generally, 21.21

Analysis of export controls

Generally, 21.22

Definition of export, 21.24

Fines and penalties for violations of Export Administration Regulations (EAR), 21.25

Items subject to Export Administration Regulations (EAR), 21.23

Publicly available software not subject to Export Administration Regulations (EAR), 21.29

Transactions subject to export controls, 21.23

Beta test software, license exception for exporting, 21.45

Classification of products for export control purposes

Generally, 21.26

CCL (see Commerce Control List (CCL), below)

Encryption, software with (see Encryption, software with, below)

Encryption, software without (see Encryption, software without, below)

Procedures for classification of products, 21.35

Commerce Control List (CCL)

Categories relevant to software companies, Export Control Classification Numbers (ECCN) for, 21.27

Country chart indicating controls applied to different countries, CCL including, 21.28

Compliance measures

Generally, 21.49

Documentation (see Documentation of export transaction, below)

Export control compliance program to document company's policies and procedures for export compliance, 21.61

Knowledge of export control violations (see Knowledge of export control violations, below)

Reporting (see Reporting and recordkeeping, below)

Development, distribution, and sales

Generally, 21.36

Cryptanalytic items, exporting limited to nongovernment end users, 21.44

Software with encryption (see Encryption, software with, below)

Software without encryption, 21.37

Documentation of export transaction

Access control system to verify address of non-U.S. party requesting software, 21.58

Automated Export System (AES) record, 21.54

Contractual certifications, third parties' agreement to comply with U.S. export control laws, 21.56

Destination control statement, 21.55

Website screening system for prospective purchasers, 21.57

Encryption, software with

Generally, 21.32, 21.38

Full encryption software, 21.35, 21.41

Limited encryption software, 21.33-21.34B, 21.41

Permitted countries, exporting encrypted software to, 21.42

Preferred countries, exporting software to, 21.41

Prohibited countries, ban on exporting encrypted software to, 21.40

U.S. subsidiaries, exporting encrypted software to, 21.39

Encryption, software without

Distribution and sales, 21.37

Hardware, software incorporated in, 21.31

Object code or source code, distinction between, 21.30

Publicly available software, 21.29

Federal agencies administering export controls, 21.21

Knowledge of export control violations

Generally, 21.50

Prohibited end users, 21.52

Prohibited end uses, 21.53

Ultimate destination of software or technology, exporter's knowledge of, 21.51

Prohibited countries

Beta test software, ban on exporting, 21.45

Encrypted software, ban on exporting, 21.40

Records (see Documentation of export transaction, above)

Related technology, export controls on, 21.48

Reporting and recordkeeping

Encryption exports reports, 21.59

Retention of records by exporter, 21.60

Sales (see Development, distribution, and sales, above)

Source code

Defined, 21.30

Encryption source code, rules for exporting, 21.46

Publicly available source code, exporting without Bureau of Industry and Security (BIS) review, 21.47

Reexport of, 21.51

Extension of Time

Patent, special act of Congress required for extending term of, 2.4

Sonny Bono Copyright Term Extension Act, extension of copyright protection under, 1.3

Fair Use Doctrine

Copyrights. See **Copyrights**

Trademarks. See **Trademarks, Service Marks, and Trade Names**

Family Entertainment and Copyright Act, 8.26B

Famous Names

Trademark protection for famous names of politicians, athletes, and celebrities, 20.30

Fanciful Marks

Likelihood of confusion in cases involving fanciful marks, factors in determining, 3.74

Fax

Order processing, 10.10

Federal Preemption. See Preemption

Federal Rules on Electronic Discovery. See Electronically Stored Information (ESI), Discovery of

Federal Trade Commission (FTC)

Children's Online Privacy Protection Act (COPPA). See **Children**

Endorsements and testimonials, 17.7A

Enforcement actions, 17.6-17.7

Gramm-Leach-Bliley Act, FTC privacy rules for financial institutions' handling of consumer information, 9.12

Privacy policies, 9.9

Websites

Bureau of Consumer Protection, 17.6

Data mining of customer information, regulation of how online businesses obtain customer's personal information, 9.8-9.9

Mail or Telephone Order Merchandise Rule, 10.16

Security measures to protect online information, 9.9A

Unwanted adware, 9.9B

Federal Trade Commission Act

Generally, 17.4

Dot com disclosure guidelines, 17.5

False or deceptive advertising, liability for, 17.4, 17.6

Fees

See also **Costs**

Attorney fees. See **Attorneys' Fees**

Co-location agreement, early termination fee provisions, 6.18

Credit card transactions, fees for, 10.3, 10.7

Debit card transactions, discount and transaction fees for, 10.4

Software license fees. See **Software License Agreements**

Software upgrade and maintenance fees, 6.42-6.43, 6.45

Trademark registration, filing fees for. See **Trademarks, Service Marks, and Trade Names**

Uniform Domain Name Dispute Resolution Policy (UDRP), arbitration fees under, 3.16

Fictitious Business Names

Trade names, protection by filing fictitious business name statements, 3.27

Fiduciary Duty

Joint owners of work, duty to account to each other for profits, 1.4

Filtering Software

Foreign countries. See **International Issues Affecting E-Businesses**

Pornography. See **Pornography**

Financial Information

California Right to Financial Privacy Act, 9.23

Financial Information Privacy Act (California), 9.22

Gramm-Leach-Bliley Act, regulation of financial institutions' handling of consumer information, 9.12

Right to Financial Privacy Act (RFPA) (Federal), 9.13

Financing Online Business

Debt financing. See **Debt Financing**

Equity financing. See **Equity Financing**

Venture capital financing. See **Venture Capital Financing**

Fines. See Penalties

First Amendment. See Freedom of Speech in Cyberspace

First Sale Doctrine

Copyrighted material, effect on, 1.23

Force Majeure Clause

Co-location agreement, 6.18

Hosting services agreement, 6.11

Foreign Laws. See International Issues Affecting E-Businesses

Forum Selection. See Choice of Forum Clause

Fraud and Misrepresentation

Choice of forum clause, effect of fraud on enforceability of, 19.12

Company privacy or data mining practices, remedies for misrepresentation of, 9.27

Computer Fraud and Abuse Act. See **Computer Fraud and Abuse Act (CFAA)**

Digital Millennium Copyright Act, safeguards against fraudulent infringement claims against internet service provider, 1.37

False or misleading advertising, laws prohibiting. See **Advertising**

Online transactions, fraud prevention tools, 10.8-10.9

Trademarks, false designation of origin, false description, or false and misleading representation of fact in connection with goods

or services, 3.61

Freedom of Speech in Cyberspace

Generally, 20.14

California Anti-SLAPP statute, 20.25

First Amendment

Generally, 20.15

Anonymous communications, free speech rights in, 20.24

Balancing of competing interests under, 20.14

Comity, effect of First Amendment on enforcement of foreign judgments, 21.5

Complaint site, protection for, 20.28

Defamation. See **Defamation**

Fighting words doctrine, inapplicability to cyberspeech, 20.15

Obscenity, lack of First Amendment protection for, 20.16

Private persons or businesses, inapplicability of First Amendment to, 20.24

Right of publicity, First Amendment defenses in action for commercial misappropriation, 20.9

Spam e-mail, applicability of First Amendment to, 20.24

Harmful matter, California Pen C §313 prohibiting distribution to minors, 20.22

Pornography. See **Child Pornography; Pornography**

Freelancers. See Independent Contractors

Freeware. See Open Source Software

Goodwill. See Trademarks, Service Marks, and Trade Names

Gripe Sites. See Complaint Sites

Guaranties. See Loans

Hacking. See Cyberattacks

Hardware

Leasing, 5.10, 16.16

Term loans for acquisition of hardware, 16.14, 16.24

Health Insurance Portability and Accountability Act (HIPPA)

Generally, 20A.2

Privacy protections for medical records, 9.10-9.11

High-Speed Internet

Co-location providers, 6.14

Vulnerability to hackers, 18.1

Hosting Agreements

Generally, 6.1

Co-location agreements distinguished, 6.14, 6.20

Customers. See **Customers**

Deadlines and turnaround times, 6.9

Electronic data discovery, use of third-party data-hosting service for, 20A.47

Exhibits

Master agreement, hosting services agreement attached as exhibit to, 6.11

Service level agreement attached as exhibit to long-form hosting or technical support agreement, 6.22

Force majeure clause, 6.11

Form of hosting services agreement, 6.11, 6.12, 6.38, 6.39

General technology companies, hosting services provided by, 5.10

License grant allowing third party to host or maintain website, 5.17

Negotiating hosting agreement, 6.2

Ownership issues, 6.8

Responsibilities of customer, 6.9

Responsibilities of host

Generally, 6.3

Content uploading and maintenance, 6.7, 6.9

Data collection and reporting, 6.8

Monitoring ongoing operations and use of hosted content, 6.5

Software access for customers or employees, 6.4, 6.6

Website hosting, 5.9, 6.4

Service credits, 6.11

Service level agreements. See **Service Level Agreements (SLAs)**

Technical support agreement. See **Technical Support**

Warranties, 6.10-6.11

Website development specialists, hosting services provided by, 5.9

Human Resources. See Employers and Employees

Hyperlinks

Digital Millennium Copyright Act, information location tools safe harbor for referring users to hyperlinks, 1.40

Ideas

Copyright protection for ideas, lack of, 1.2

Identity Theft

See also **Privacy**

Methods of combating, website for, 9.2

Notice of security breach leading to possible identity theft, 18.15

Office of Privacy Protection, website for, 9.3

Immunity

Digital Millennium Copyright Act, immunity of service providers for passive copyright infringement under. See **Digital Millennium Copyright Act (DMCA)**

ISP's immunity under Communication Decency Act. See **Defamation**

Indemnification

Website developer, indemnification agreement covering claims for infringement of patents, copyrights, and third party intellectual property rights, 3.78

Independent Contractors

Consulting agreement, sample form, 4.19

Distinguishing between contractors and employees

Generally, 4.13

Behavioral control, 4.15

Classification overview, 4.14

Financial control, 4.16

Type of relationship, factors considered by IRS, 4.17

Intellectual property created by independent contractors, 4.18

Joint works, 4.18

Nondisclosure agreements, 4.20, 4.21

Website developers

Generally, 5.4

Advantages of using freelancers, 5.8

Agreements for independent contractors, contents of, 5.23

Intellectual property created by independent contractors providing value inherent in business's website, 5.1

Ongoing obligations of, 5.22

Presumption of ownership in favor of independent contractor, 5.6, 5.11-5.12, 5.17

Work made for hire doctrine, applicability of, 5.12

Work made for hire

Factors in determining if work qualifies as, 1.5

Website developers, applicability of work made for hire doctrine, 5.12

Inferences. See Presumptions and Inferences

Infringement (Generally)

Content of website, exemption from infringement liability. See **Content of Website, Obtaining Licenses and Rights to Use**

Copyrights. See **Infringement of Copyright**

Domain names. See **Domain Names**

Patents. See **Patents**

Specialized software under license, warranty against infringement of, 6.10

Trade dress. See **Trade Dress**

Trademarks. See **Trademarks, Service Marks, and Trade Names**

Infringement of Copyright

See also **Copyrights**

Generally, 1.12

Attorney fees and costs

Digital Millennium Copyright Act, recovery of fees and costs for misrepresentations in notification of infringement, 1.37

Owner's entitlement to, 1.17

Contributory copyright infringement (see Direct, contributory, and vicarious copyright infringement, below)

Copies of computer programs, safe harbor for, 1.16B

Costs (see Attorney fees and costs, above)

Criminal liability for, 1.17

Direct, contributory, and vicarious copyright infringement

Generally, 1.13

Actual or constructive knowledge by defendant of direct infringement by third parties as requirement for establishing contributory infringement, 1.15

Digital Millennium Copyright Act, immunity of internet service providers under. See **Digital Millennium Copyright Act (DMCA)**

Doctrine of vicarious infringement, 1.16

Establishing direct infringement liability of ISP or BBS, requirement for, 1.14

Inducement, 1.16A

Prima facie case of direct copyright infringement, plaintiff establishing, 1.12

Downloading and uploading content as copyright infringement, 8.20

Encryption software for shielding service provider from knowledge of users' copyright infringement, 8.27

Fair use defense to copyright infringement claim, 8.27, 14.6

Family Entertainment and Copyright Act, investigation and conviction of file swappers for infringing activities under, 8.26B

Indemnification agreement with website developer covering infringement claims, 3.78

Innocent infringement, 1.7

Insurance coverage for infringement claim, 20.39

Internet service providers. **Internet Service Providers (ISP)**

Linking arrangements, copyright infringement issues associated with, 8.16

No Electronic Theft Law (NET Act), criminal prosecution for sound recording infringements under, 8.26

Notice of copyright, effect on defense based on innocent infringement, 1.7

Registration of copyright

Damages, recovery for infringement of registered copyright, 1.17

Preregistration of works under Artists' Rights and Theft Protection Act of 2005 (ART Act), 1.8C

Prerequisite for infringement suit, registration of copyright as, 1.8

Remedies for, 1.17

Substantial similarity between works, two-part test for establishing, 1.12

Vicarious copyright infringement (see Direct, contributory, and vicarious copyright infringement, above)

Website user interface, effect of copying, 3.78

Injunctions

Anticybersquatting Consumer Protection Act (ACPA), injunctive relief under, 3.24

Computer Fraud and Abuse Act, injunctive relief under, 17.28

Copyright infringement, injunction against, 1.17

False or misleading advertising claims, injunctive relief for, 17.6, 17.9

Phishing violations, injunctive relief for, 9.6C

Trademarks, injunction against infringement of. See **Trademarks, Service Marks, and Trade Names**

Trade secrets, injunction to protect, 2.26, 2.34

Trespass to chattels theory, obtaining preliminary injunction on, 18.18

Installment Payments

Promissory note, principal payments made in fixed periodic installments, 16.25

Software license fees paid in installments, 12.5

Insurance for On-Line Businesses

Generally, 20.34

Business interruption coverage, 20.40

Co-location facility, insurance coverage for equipment located at, 6.20

Commercial general liability insurance

New endorsements and policy language excluding e-commerce related risks, 20.41

Tangible property, coverage for damage to, 20.35

Comprehensive general liability insurance

Generally, 20.35

Intellectual property infringement claims, coverage for, 20.39

Physical loss or damage, loss of computer data constituting, 20.38

Tangible property (see Tangible property, loss of, below)

Third party and first party coverage distinguished, 20.35

Electronic data defined, 20.41

Exclusions and gaps in coverage, review of policies to determine, 20.42

Purchase of separate policy or endorsement to cover potential claims relating to online business activities, 20.42

Tangible property, loss of

Coverage for loss of computer data, 20.36

Damage to tangible property, coverage for, 20.35

Distinction between actual loss of data and loss of benefit related to data, 20.37

Term sheet for preferred stock financing, key-man insurance provisions in, 16.10

Intellectual Property

Acquisition of, generally, 5.1

Agreement for transfer and assignment of intellectual property, 5.3

Assignment of intellectual property, generally, 5.1-5.2, 5.3

Coding. See **Coding**

Comprehensive general liability insurance policy, coverage for infringement claim under, 20.39

Contents of websites. See **Content of Website, Obtaining Licenses and Rights to Use**

Copyrights. See **Copyrights**

Defined, 16.26

Domain names. See **Domain Names**

Due diligence procedures. See **Acquisitions and Sales of Internet-Based Businesses**

Exclusive licenses. See **Licenses**

Forensic images, collection of, 20A.37

Owners of intellectual property, identifying, 14.7

Patents. See **Patents**

Representations and warranties, intellectual property in purchase agreement, 22.1, 22.3, 22.16, 22.17

Security interests in intellectual property collateral, financing business through. See **Debt Financing**

Service marks. See **Trademarks, Service Marks, and Trade Names**

Trademarks and trade names. See **Trademarks, Service Marks, and Trade Names**

Trade secrets. See **Trade Secrets**

Venture capital financing agreements including proprietary information and inventions agreement, 16.8

Vesting of rights to intellectual property, 5.1

Websites. See **Website Development**

World Intellectual Property Organization. See **World Intellectual Property Organization (WIPO)**

Interest on Money

London Interbank Offered Rate (LIBOR), 16.24

Maximum permissible interest rate, 16.22

Promissory note, payment of principal and interest under, 16.25

International Issues Affecting E-Businesses

See also **European Union Directives**

Generally, 21.1

Advertising on Internet involving commerce with foreign nations, FTC's limited jurisdiction over, 17.4

Applicable law in international disputes, 21.3

Comity, enforcement of foreign judgments against U.S. companies, 21.5

Contracts

Electronic contracting (see Electronic contracting, below)

World Intellectual Property Organization (WIPO), model contract clauses requiring submission of disputes to mediation or arbitration by, 21.9

Electronic contracting

Convention on the Use of Electronic Communications in International Contracting, 21.8

European Union directives on enforceability of, 7.13

Export controls on software. See **Export Controls on Commercial Software and Technology**

Filtering of Internet

Content of Internet, foreign governments' filtering of, 21.6

Geo-filtering software, identifying home country of Internet address by using, 21.7

Hague Conference on Private International Law, proposed Convention on Exclusive Choice of Court Agreements, 21.2

Jurisdiction of foreign courts over online business activities, 21.4

Limiting geographical scope of markets target by company's website, 21.7

Madrid Protocol, obtaining trademark protection in foreign countries under, 3.48

Online businesses' liability based on foreign laws, 19.18

Patents, distinction between U.S. and international law, 2.14

Self-regulation of online businesses

Alternate dispute resolution, 21.20

Trustmark on websites certify subscribing businesses' adherence to certain business standards, 21.19

Shopping cart service, accommodation of foreign languages or currencies by, 10.13

Tax policy affecting international e-commerce, 10.18

World Intellectual Property Organization. See **World Intellectual Property Organization (WIPO)**

Internet Service Providers (ISPs)

Copyright infringement, liability of ISP for. See **Digital Millennium Copyright Act (DMCA)**

Defamation by subscribers, ISP's liability for. See **Defamation**

Defined, 1.30

Direct infringement liability of ISP, requirement for establishing, 1.14

Hosting agreements. See **Hosting Agreements**

Internet Tax Freedom Act (ITFA), 10.17-10.18, 10.20

Interpretation of Statutory and Case Law. See Construction and Interpretation

Interruption of Business

Insurance coverage for, 20.40

Interstate Commerce

Child Pornography Prevention Act (CPPA), distributing child pornography in interstate commerce prohibited under, 20.19

Obscene materials, federal law prohibiting transportation of, 20.16

Invention Assignment Agreements. See Confidentiality and Invention Assignment Agreements

Inventions. See Patents

Inventory

Website development, inventory of intellectual property needed for, 5.1

Investors

Angel investors, 16.3, 16.6, 16.34

Debt financing. See **Debt Financing**

ISPs. See Internet Service Providers (ISPs)

ITFA. See Internet Tax Freedom Act (ITFA)

Joint Works. See Copyrights

Judgments and Decrees

Default judgments. See **Default and Default Judgments**

Foreign judgment, enforcement against U.S. companies, 21.5

Junk E-Mail. See Spam E-Mail

Jurisdiction

See also **Venue**

Generally, 19.1

Advertising on Internet, FTC jurisdiction over, 17.4

Anticybersquatting Consumer Protection Act, in rem jurisdiction over domain name, 19.11

CAN-SPAM Act, FTC's jurisdiction to enforce, 17.22

Choice of forum. See **Choice of Forum Clause**

Conflicts of law. See **Conflicts of Law**

Constitutional limits on personal jurisdiction

Due process (see Due process clause of US Constitution, below)

Minimum contacts test, 19.6

Reasonableness requirement for court's exercise of jurisdiction, 19.7

Definitions, 19.1

Due process clause of US Constitution

Limits on jurisdiction, due process clause establishing, 19.5

Specific personal jurisdiction, due process clause permitting, 19.9

Federal subject matter jurisdiction, types of, 19.2

Foreign courts' jurisdiction over online business activities, 21.4

In rem jurisdiction, 19.11

Personal jurisdiction

Generally, 19.2

Constitutional limits (see Constitutional limits on personal jurisdiction, above)

Federal Rules of Civil Procedure, federal courts exercising personal jurisdiction under, 19.4

General personal jurisdiction, standards for asserting, 19.8

Long-arm statute allowing courts to exercise personal jurisdiction over nonresidents, 19.3

Specific personal jurisdiction for particular claim, 19.9

Specific personal jurisdiction in cyberspace, 19.10

Sales and use taxes on e-commerce transactions, jurisdictional issues on imposition of, 10.22-10.23

Terms of use policy, jurisdictional issues addressed in, 8.3

Lanham Act

Generally, 3.26

Advertising on Internet, provisions regarding, 17.3

Intent-to-use applications, prohibition on assignments of, 16.29

Trade dress. See **Trade Dress**

Trademarks. See **Trademarks, Service Marks, and Trade Names**

Law Enforcement Personnel

Digital Millennium Copyright Act (DMCA), exceptions to anti-circumvention provisions for authorized activities of law enforcement, intelligence gathering, and other governmental activities, 1.26

Leases

Capital leases, 16.16

Co-location agreement, equipment leasing provisions, 6.20

Hardware, leasing, 5.10, 16.16

Operating leases, 16.16

Legislative Intent

CAN-SPAM Act, 17.12

Letter of Intent

Confidentiality provisions, effect of, 16.10

Strategic alliance, letter of intent, 11.3

Letters

Advisory board letter agreement, 4.23

Cease and desist letters, 3.69, 3.70, 20.33

Intent re strategic alliance, sample letter, 11.3

Legal hold letter to client, 20A.23, 20A.24

Letter of intent. See **Letter of Intent**

Litigation hold letter to opponent, 20A.25, 20A.26

Offer letter to prospective employees, 4.4, 4.5

Preservation-of-evidence letter, 20A.25

Spoliation letter, 20A.25

Libel. See Defamation

Libraries

Filtering software. See **Pornography**

First Amendment considerations affecting libraries' installation of blocking software to prevent minors access to pornographic materials, 20.15

Licenses

Contents of website, obtaining license to. See **Content of Website, Obtaining Licenses and Rights to Use**

Copyrights. See **Copyrights**

Derivative works, license to authorize reproduction, distribution, and preparation of, 6.9

Digital reprint rights license, 14.13, 14.14

Export licenses. See **Export Controls on Commercial Software and Technology**

Hosting agreement, license grant included in, 6.9

Intellectual property licenses, exclusivity of

Generally, 5.1, 5.19

Software license agreements. See **Software License Agreements**

Patent license, termination of payment obligations after expiration of patent, 2.4

Source code license instead of source code escrow, 15.1

Website development agreements, ownership and license grants within, 5.17-5.20

Likelihood of Confusion. See Metatags; Trademarks, Service Marks, and Trade Names

Limitation of Actions. See Statutes of Limitations

Limited Liability Companies (LLCs)

Disadvantages of, 16.2

Ownership interests in LLCs, 16.2

Linking Arrangements

Generally, 8.14

Agreement, 8.18

Copyright infringement issues, 8.16

Deep linking, 8.15

Definition of link, 8.15

Framing, 8.15

Image link, 8.15

Inline link, 8.15

Out link, 8.15

Trespass to chattels, potential liability for, 8.17

Liquidation

Term sheet for preferred stock financing, liquidation provision in, 16.10

Litigation Hold. See Electronically Stored Information (ESI), Discovery of

LLCs. See Limited Liability Companies (LLCs)

Loans

Bridge loans, 16.3, 16.7, 16.34

Contents of loan or credit agreement, 16.21

Debt financing of online business. See **Debt Financing**

Guaranties

Personal guaranties of company's loan obligations, 16.21

Small Business Administration, loans and loan guaranties by, 16.15

Hardware, term loans for acquisition of, 16.14, 16.24

Negative loan covenants, effect of, 16.24

Usury, 16.22

Waiver of reporting provisions in loan agreement, 16.24

Madrid Protocol

Trademark protection in foreign countries, obtaining under Madrid Protocol, 3.48

Marketing

See also **Advertising**

Copyrighted work, effect of fair use on potential market or on value of, 1.22

Directing marketing disclosures of customers' personal information, application of Civil Code §1798.83, 9.26

Domain name registration as part of marketing efforts, 3.1

Foreign countries, limiting geographical scope of markets target by company's website, 21.7

FTC publication, Advertising and Marketing on the Internet: Rules of the Road, 17.5

Interactive marketing agreement, 17.35, 17.36

Strategic alliances. See **Strategic Alliances**

Mediation. See Arbitration

Metatags

Generally, 3.71

Advertising, metatags as form of, 17.1

Initial interest confusion test to determine if metatags infringing on trademark, 3.73

Lanham Act violation, using third party's trademark as metatag constituting, 3.71

Likelihood of confusion

Fanciful marks, factors in evaluating likelihood of confusion in cases involving, 3.74

Generic English words or trademarks, effect of using in banner ads, 3.76

Third party's trademarks as metatags, applicability of test to use of, 3.71

Misspelling of trademark as metatag constituting misappropriation of competitor's goodwill, 3.75

Nominative fair use of trademark in metatag as defense to infringement claim, 3.72

Mining Customer Data. See Privacy

Minors. See Children

Misappropriation of Trade Secrets. See Trade Secrets

Misrepresentations. See Fraud and Misrepresentation

Modifications. See Amendments and Modifications

Mousetrapping, 17.7

Music on Internet

Generally, 8.21

Burning CDs, 8.22

Case law, 8.27

De minimis copying defense, 14.17

Downloading, 8.22

Fair use defense to copyright infringement claim, 8.27

Federal statutes

Generally, 8.23

Audio Home Recording Act of 1992 (AHRA), 8.24, 8.27

Digital Performance Right in Sound Recordings Act of 1995 (DPRA), 8.25, 8.27

Family Entertainment and Copyright Act, 8.26B

No Electronic Theft Law (NET Act), 8.26

Pen C §653aa (Internet piracy), 8.26A

Licensing music, 14.17

MP3 files, 8.22, 8.27

Recording Industry Association of America (RIAA) litigation strategy, 8.28

Ripping, 8.22

Sampling of musical compositions, 14.17

Space-shifting files, 8.27

Streaming audio, 8.22, 8.27

Watermark technologies, 8.22

Names

Domain names. See **Domain Names**

Fictitious business names. See **Fictitious Business Names**

Trade names. See **Trademarks, Service Marks, and Trade Names**

Negotiations

Acquisitions and sales of Internet-based businesses, preliminary issues before entering negotiations, 22.1

Attorney working with company founders and executives, ethical considerations and conflicts of interest in employment negotiations, 4.2

Co-location agreements, negotiability of, 6.18

Hosting agreement, 6.2

Representations and warranties, negotiation of, 6.10, 6.17

Website development agreements, role of attorney in drafting and negotiating, 5.1, 5.5-5.6

Networks

Denial of service attacks on networks, 18.1

Electronic evidence, up-to-date maps of computer networks as useful in narrowing search for information, 20A.29

Peer-to-peer networks, 8.14

Point-of-sale (POS) networks, online debit transactions conducted over, 10.4

Service level agreements shifting risk of network failures and downtime to service providers, 6.23

Testing and monitoring of networks, 6.24

Wireless networks. See **Wireless Networks and Devices**

No Electronic Theft Law (NET Act), 8.26

Nondisclosure Agreements

See also **Confidentiality and Invention Assignment Agreements**

Independent contractors, 4.20, 4.21

Trade secrets, nondisclosure agreement to protect, 2.25, 2.32, 2.33, 2.37

Nonresidents, Jurisdiction Over. See Jurisdiction

Notary Public

Trademark assignment, notarial acknowledgment as prima facie evidence of, 3.57

Notes. See Promissory Notes

Notice and Notification

Banner advertising agreement, notice of termination for, 17.32

Browse-wrap agreements, notice requirements, 7.4

CAN-SPAM Act, notice of opt-out options, 17.14, 17.16

Constructive notice. See **Constructive Notice**

Copyright notice, benefits of, 1.7

Digital Millennium Copyright Act, notifying ISP of copyright infringement. See **Digital Millennium Copyright Act (DMCA)**

Duty to preserve data, notice of pending litigation triggering, 20A.21-20A.22

FTC's Mail or Telephone Order Merchandise Rule, notice of inability to timely ship product under, 10.16

Hosting agreement, notice of termination of, 6.10

Security breaches, notice of, 9.24-9.25, 18.15

Service level agreements, notifying provider of service problems under, 6.27-6.29

Trademark, notice of opposition to registration of, 3.49

Obscenity

See also **Pornography; Sexually Oriented Materials**

Generally, 20.16

First Amendment protection for obscenity, lack of, 20.16

Offer Letter to Prospective Employees, 4.4, 4.5

Officers. See Directors and Officers

Online Privacy Protection Act. See Privacy

Online Software License Agreements. See Software License Agreements

Open Source Software

Advantages of, 8.8, 22.13A

Berkeley Software Distribution (BSD), 8.8

Checklist for acquiring open source software, 22.13B

Open Source Initiative, 8.8

Open source software license agreement, 8.8, 8.9

Operating Systems

Denial of service attacks on operating systems, 18.1

Opinions

Qualified privilege for expressions of opinion, 20.3, 20.15

Orders

Consent order, civil penalties or injunction sought by FTC for company's violation of, 17.6

Protective orders. See **Protective Orders**

Organization for Economic Cooperation and Development (OECD)

International e-commerce tax policy addressed by OECD, 10.18

Other States

Data protection programs in other states, 9.27A

Sales by out-of-state vendors, laws governing, 17.10

Outsourcing

Service level agreements in outsourcing arrangements, importance of, 6.22

Overtime

Special rules for computer programmers, 4.12

Ownership and Possession

Copyrights, ownership of. See **Copyrights**

Corporation, ownership interests, 16.2

Domain names. See **Domain Names**

Equity financing. See **Equity Financing**

Hosting agreements, addressing ownership issues in, 6.8

Intellectual property, identifying owners of, 14.7

Invention assignment agreement. See **Confidentiality and Invention Assignment Agreements**

LLC, ownership interest in, 16.2

Software, effect of purchase of code on ownership rights, 12.1

Trademark, ownership based on priority of use, 3.29

Venture capital financing, dilution of ownership, 16.7, 16.10

Website development, ownership issues. See **Website Development**

Parents. See Children

Patents

Generally, 2.1

Abstract ideas, unpatentability of, 2.3

Administration of patents by United States Patent and Trademark Office, 2.2

Application for patent

Generally, 2.10

Appeal of rejected patent application, 2.10

Best mode or version of claim invention, applicant's disclosure of, 2.11

Claims regarding subject matter of invention, inventor's patent rights defined by, 2.12

Disclosure requirements in patent application, 2.11

Exclusive license to whole or part of patent application, applicant, patentee, or assigns granting, 2.15

Joint applications by co-inventors, 2.6

Patent examiner, assignment of application to, 2.10

Pre-application activities preventing approval of application, 2.13

Specification and enablement requirements distinguished, 2.11

Statutory time bars, 2.13

Subject matter of application, patent application filed by inventor of, 2.6

Written description of claimed invention, requirement of, 2.11

Assignment of patent (see Transfer of patent, below)

Business method patents, 2.1, 2.18

Constitutional basis for patents, 2.2

Defined, 2.1-2.2

Design patents

Generally, 2.3

Term of, 2.4

Extension of patent, special act of Congress required for, 2.4

Infringement of patent

Claims in patent application, infringement action focusing on construction and interpretation of, 2.12

Indemnification agreement with website developer covering infringement claims, 3.78

Treble damages, recovery of, 2.2

Unlicensed software use as, 14.4

International patent law and U.S. patent law distinguished, 2.14

Internet-related patents, list of, 2.18

Licenses

Exclusive license to whole or part of patent or patent application, applicant, patentee, or assigns granting, 2.15

Nonexclusive licenses of patents, 2.15

Termination of payment obligations after expiration of patent, 2.4

Litigation issues, 2.17A

Mathematical algorithms, patentability of, 2.3, 2.19

Patent prosecution, 2.10

Plant patents

Generally, 2.3

Term of, 2.4

Recordation of documents. See **Recordation of Documents**

Registration of patent, 5.1

Requirements for patentability

Generally, 2.5

Inventor of subject matter of application, patent application filed by, 2.6

Nonobviousness of differences between subject matter of patent and prior art, effect of, 2.9

Novelty of process or product, 2.8

Subject matter requirements, 2.3

Unpatentable subject matter, 2.3

Utility of invention, 2.7

Security interests in patents, perfecting, 16.28

Software patents

Generally, 2.19

Application for patent, best mode for software-related inventions, 2.11

Term of patents, 2.4

Trade dress distinguished, 3.80

Trade secret protection as alternative to patent, 2.4

Transfer of patent

Generally, 2.15, 16.28

Form of patent assignment, 2.16

Licensing patent, 2.15

US Patent & Trademark Office cover sheet, 2.17

Types of patents, 2.3

Utility patents

Generally, 2.3

Term of, 2.4

World Intellectual Property Organization (WIPO), alternative dispute resolution services offered by, 21.9

Patriot Act. See USA Patriot Act

Payments. See E-Commerce Transactions and Payments

PayPal, 10.6

Penalties

California's anti-spam law, penalties for violations for, 17.25

CAN-SPAM Act violations, 17.20, 17.22

Children's Online Privacy Protection Act (COPPA), 9.33

Computer Fraud and Abuse Act (CFAA), penalties and private right of civil action under, 9.14

Criminal penalties. See **Criminal Law**

Digital Millennium Copyright Act, civil damage penalties for misrepresentations in notification of infringement under, 1.37

Discovery of electronically stored information, penalties for failure to comply with rules regarding. See **Electronically Stored Information (ESI), Discovery of**

Electronic Communications Privacy Act (ECPA), 9.15, 18.8

Export Administration Regulations (EAR), fines and penalties for violations of, 21.25

False or deceptive advertising, FTC penalties for, 17.6

FTC's Mail or Telephone Order Merchandise Rule, penalties for violations of, 10.16

Hacking, penalties for, 17.27, 18.16

Prepaid loans, penalties for, 16.24

Pending Litigation

Discovery of electronically stored information (ESI) when litigation pending. See **Electronically Stored Information (ESI), Discovery of**

Personal Jurisdiction. See Jurisdiction

Phishing, 3.63, 9.6C

Photographs

Copyright protection for, Generally, 14.3

Still photograph license, obtaining before launch of website, 14.11, 14.12

Plant Patents. See Patents

Pop-Up Ads, 17.1

Pornography

See also **Child Pornography; Obscenity; Sexually Oriented Materials**

Filtering software

Children's Internet Protection Act (CIPA), filtering of Internet sites by public schools and libraries, 20.21

First Amendment issues involving, 20.23

Server-side versus client-side filtering software, 20.23

Harmful matter, Pen C §313 prohibiting distribution to minors, 20.22

Portal Agreements, 17.35, 17.36

Preemption

CAN-SPAM Act, preemption of state law by, 17.12, 17.25-17.26

Communications Decency Act (CDA), preemption of state law under, 20.7

Health Insurance Portability and Accountability Act (HIPPA), no preemption of state privacy protections, 9.10

Lanham Act, no preemption of UCC by, 16.29

Uniform Electronic Transactions Act (UETA), preemption by E-Sign, 7.9

Presumptions and Inferences

At will employment, 4.3

Intellectual property ownership, presumption in absence of written agreement, 5.6, 5.11-5.12, 5.17

Uniform Electronic Transactions Act (UETA), inferred agreement to conduct transaction electronically under, 7.10

Privacy

See also **Confidentiality; Disclosure; Identity Theft; Tracking Software**

Generally, 9.1

Better Business Bureau's privacy seal indicating business' adherence to online Privacy Participation Agreement, 21.19

California privacy laws

Generally, 9.18

Anti-paparazzi statute, 9.21A

California constitution, 9.16

Common law right, 9.17

Consumer Protection Against Spyware Act, prohibitions under, 9.26A

Directing marketing disclosures of customers' information, application of CC §1798.83, 9.26

Financial Information Privacy Act, 9.22

Online Privacy Protection (see Online Privacy Protection Act, below)

Right to Privacy Act (California), 9.23

Children's Online Privacy Protection. See **Children**

Constitutional law

California constitutional protections, 9.16

U.S. constitutional protections, 9.7

Cookies. See **Cookies**

Customer personal information, data mining by online businesses

Generally, 9.2

Cookies, 9.4

Developing company privacy policies and safeguards for customer information, 9.1

Tracking software. See **Tracking Software**

Voluntary disclosure, 9.3

Web bugs, 9.5

Data mining

Customer personal information (see Customer personal information, data mining by online businesses, above)

Liability for company's failure to adhere to privacy policy or to disclose consumer data mining activities, 9.9

Electronic Communications Privacy Act. See **Electronic Communications Privacy Act (ECPA)**

E-mail, no expectation of privacy for employees using, 20A.5

European Union Directives. See **European Union Directives**

Federal privacy laws

Generally, 9.8

Computer Fraud and Abuse Act. See **Computer Fraud and Abuse Act (CFAA)**

Electronic Communications Privacy Act. See **Electronic Communications Privacy Act (ECPA)**

E-mail, searches by employer, 9.15

FTC initiatives, 9.8-9.9B

Gramm-Leach-Bliley Act, regulation of financial institutions, 9.12

Right to Financial Privacy Act (Federal), 9.13

U.S. Constitution, 9.7

Health Insurance Portability and Accountability Act (HIPPA), protection of medical information, 9.10-9.11

Online Privacy Protection Act

Contents of privacy policy, requirements for, 9.20

Failure to comply, 9.21

Posting of privacy policy required, 9.19

Other states' data protection programs, 9.27A

Privacy policy statements, 7.4

Publicity, right of, 20.9

Security breaches, notice of, 9.24-9.25, 18.15

Self-regulation, 9.2, 9.8

Tracking software, invasions of privacy through. See **Tracking Software**

Unfair business practices, 9.27

Website privacy policies

Basic website policy, sample form, 9.43, 9.44

Certification from nonprofit privacy organization, privacy seal program, 9.42

Commercial website policy, sample form, 9.45, 9.46

Content of policies, 9.40

Enforceability of policies, 9.41

Need for, 9.39

Opt-in and opt-out procedures, 9.40

Resources for preparation of policies, 9.42

Watchdogs, 9.42

Privileges

Attorney-client privilege. See **Attorney-Client Privilege**

Electronically stored information (ESI) as privileged material. See **Electronically Stored Information (ESI), Discovery of**

Opinions, qualify privilege for, 20.3, 20.15

Trade secret privilege, party asserting during litigation, 2.37

Work product privilege. See **Work Product Privilege**

Production of Electronic Evidence. See Electronically Stored Information (ESI), Discovery of

Profits

Joint owners of work, duty to account to each other for profits, 1.4

Trademark infringement action, recovery of defendant's profits in, 3.63

Programs. See Software

Promissory Notes

Generally, 16.21

Convertible promissory notes

Generally, 16.34

Form, 16.35

Form of promissory note, 16.23, 16.25, 16.35

Proof

See also **Burden of Proof; Evidence**

Anticybersquatting Consumer Protection Act (ACPA), proving cause of action for damages under, 3.23

Browse-wrap agreement, proof required for enforcement of, 7.4

European Union Directive requiring manufactures to provide proof of conformity with minimum safety requirements, 21.17

Protective Orders

Injunctions. See **Injunctions**

Trade secrets, protective order to prevent disclosure during litigation, 2.37

Public Domain

Expired copyright, effect of using work with, 14.5

Restoring copyright in works previously in public domain, 1.3

Public Entities and Employees

Digital Millennium Copyright Act (DMCA), exceptions to anti-circumvention provisions for authorized activities of law enforcement, intelligence gathering, and other governmental activities, 1.26

Publicity, Right of

Common law right of, 20.9

Public Policy

Choice of forum clause, public policy exception to enforceability of, 19.12

Employee mobility, public policy favoring, 2.26

Punitive Damages

Trade secret misappropriation, recovery of punitive damages for, 2.36

Questionnaires. See Charts, Checklists, Questionnaires, and Tables

Questions of Law and Fact

Novelty of invention as question of fact, 2.8

Trademark, abandonment as question of fact, 3.53

Recordation of Documents

Copyright transfer, recordation of, 1.9, 16.27

Intellectual property, recording assignment of, 5.1

Patents

Assignment document, recordation of, 2.15

Security interest in patent, discretionary recording of, 16.28

Records and Reports

Automated Export System (AES) record, 21.54

Child pornography, ISP reporting, 20.13

Copyright registration as public record of copyright claim, 1.8

Discovery of electronically stored information (ESI). See **Electronically Stored Information (ESI), Discovery of**

Due diligence report for acquisition and sale of Internet-based business, 22.9, 22.14, 22.15

E-Sign, retention and evidentiary use of electronic records under, 7.7-7.8

Export documentation. See **Export Controls on Commercial Software and Technology**

Financial records, right to privacy, 9.12-9.13

Health Insurance Portability and Accountability Act (HIPPA), privacy of medical information, 9.10-9.11

Loan agreement, waiver of reporting provisions in, 16.24

Service level agreement, reports detailing service provider's performance under, 6.35-6.36

Software license agreement, reporting requirements for royalties, 12.12

Technical support services agreement, reporting requirements, 6.43

Trademark registrations, Secretary of State's office maintaining records of, 3.31

Uniform Electronic Transactions Act (UETA), retention and evidentiary use of electronic contracts under, 7.9

Video rental records, online data mining of customer information, 9.8

Redemption

Term sheet for preferred stock financing, redemption provision in, 16.10

Referral Sites. See Service Directories or Referral Sites

Refunds

FTC's Mail or Telephone Order Merchandise Rule, refunds under, 10.16

Registration

Copyright registration. See **Copyrights**

Domain names, registration of. See **Domain Names**

Term sheet for preferred stock financing, registration rights provision in, 16.10

Trade dress, registration with U.S. Patent and Trademark Office, 3.77

Representations and Warranties

American Law Institute (ALI) software contract principles, implied warranty under, 7.12

Co-location agreements. See **Co-Location Agreements**

Disclaimers

Co-location agreement, disclaimer of warranties under, 6.18

Hosting agreement, disclaimer of warranties by customers, 6.10-6.11

Software license agreements, disclaimer of implied warranties in, 8.4

Drafting considerations for electronic contracts, generally, 7.14

Hosting agreements, 6.10-6.11

Industry standard warranty providing that servers and software free from viruses and harmful code, 6.10

Infringement of specialized software under license, warranty against, 6.10

Intellectual property, purchase agreement's representations and warranties re, 22.1, 22.3, 22.16, 22.17

Negotiation of, 6.10, 6.17

Service level agreement compared, 6.10, 6.17

Software license agreements, warranty provisions, 8.4, 12.7, 12.12

Term sheet for preferred stock financing, representations and warranties in, 16.10

Website development agreement, developer's representations and warranties in, 5.21-5.22

Reprints

Generally, 1.6

Digital reprint rights license, 14.13, 14.14

Reputation

Libel, definition of, 20.2

Retention of Electronically Stored Information (ESI). See Electronically Stored Information (ESI), Discovery of

Reverse Engineering

Defined, 2.24

Digital Millennium Copyright Act (DMCA), exceptions to anti-circumvention provisions for reverse engineering, 1.26

Software license agreements, prohibition on reverse engineering under, 8.4

Trade secrets

Discovery of trade secret by reverse engineering, 2.24

Misappropriation of trade secrets, reverse engineering as defense to claim of, 2.35

Royalties

Definition of royalty base, 12.5

Independent contractors, 4.18

Software license agreements. See **Software License Agreements**

Trade secret misappropriation, plaintiff's election to receive reasonable royalty in lieu of damages for, 2.36

Safe Harbors

Children's Online Privacy Protection Act (COPPA), safe harbor from parental consent requirement, 9.34

Digital Millennium Copyright Act. See **Digital Millennium Copyright Act (DMCA)**

Electronically stored information (ESI), safe harbors regarding discovery of, 20A.11, 20A.15

European Union Directives. See **European Union Directives**

Internet service providers (ISPs), safe harbors limiting liability for copyright infringement. See **Digital Millennium Copyright Act (DMCA)**

Safety

European Union Directive requiring manufactures to provide proof of conformity with minimum safety requirements, 21.17

Sale of Business. See Acquisitions and Sales of Internet-Based Businesses

Sale of Goods

Export controls. See **Export Controls on Commercial Software and Technology**

Value Added Taxes (VAT), EU requiring non-EU vendors of digital products to charge on Internet sales to EU consumers, 21.16

Sales and Use Taxes

Generally, 10.22

California sales and use taxes

Generally, 10.24

Software and related services, treatment of, 10.25

Constitutionality of state-imposed use taxes, 10.23

Discriminatory taxes on Internet access and online computer services, 10.24

Internet Tax Freedom Act (ITFA), effect of, 10.20

Jurisdictional issues, 10.22-10.23

Streamlined Sales Tax Agreement, effect of, 10.20A

Streamlined Sales Tax Project, 10.17

Sanctions. See Penalties

Sarbanes-Oxley Act, 20A.2

SBA. See Small Business Administration (SBA)

Schools

Filtering software. See **Pornography**

First Amendment considerations affecting public schools' installation of blocking software to prevent minors access to pornographic materials, 20.15

Search Engines

Digital Millennium Copyright Act, information location tools safe harbor for referring users to hyperlinks, 1.40

Metatags. See **Metatags**

Search engine optimization (SEO), 17.29A-17.29B

Trademarks. See **Trademarks, Service Marks, and Trade Names**

Trespass to chattels, use of automated search engines to collect information from websites as, 8.17

Search Warrants

Right to Financial Privacy Act (Federal and California), disclosure in response to subpoena or search warrant, 9.13, 9.23

Secondary Meaning

Trade dress. See **Trade Dress**

Trademark, secondary meaning as prerequisite for registration of nondistinctive, 3.34

Secure Transaction Processing Software

Credit card transactions, 10.3, 10.8

Encryption software. See **Encryption Software**

Securities Laws

Exemptions from, 16.22

Promissory note convertible into equity security, treatment under securities laws, 16.34

Start-up companies' compliance with securities laws, 16.5

Term sheet for preferred stock financing, registration rights provision in, 16.10

Security Breaches

Notice to customers of, 9.24-9.25, 18.15

Security Certificates, 10.11

Security Interests. See Debt Financing

Self-Regulation of Online Businesses. See International Issues Affecting E-Businesses

Servers

Co-location services, 6.13, 6.15-6.16

Electronic data discovery, secured servers used for, 20A.48

Secure server connection, URL in browser indicating, 10.8

Service Credits

Hosting agreements, 6.11

Service level agreements, 6.17, 6.24, 6.30-6.31

Service Directories or Referral Sites, 17.33

Service Disruptions

Penal Code §502, penalties for service disruptions under, 17.27, 18.16

Service Level Agreements (SLAs)

Generally, 6.21

Additional terms, generally, 6.32

Application service provider (ASP), applicability of SLA to, 6.23

Co-location provider committing to certain level of service under SLA, 6.17

Content, 6.22

Customer support. See **Customers**

Defined, 6.1, 6.21

Form of agreement

Short form service level agreement, 6.36, 6.37

Website hosting service level agreement, 6.38, 6.39

Maintenance parameters, disclosure of, 6.25

Monitoring and enforcement of SLA terms, 6.5, 6.24, 6.36

Network failures and downtime, shifting risk to service providers, 6.23

Performance measurement, 6.22, 6.24, 6.34

Reporting, 6.35-6.36

Requesting SLA, time for, 6.23

Response times and response actions, 6.24, 6.27-6.30

Self-executing nature of remedies under SLA, 6.10, 6.17

Service credits and chronic problems, 6.17, 6.24, 6.30-6.31

Service levels

Generally, 6.24, 6.26

High priority (Priority One) requests, 6.29

Low priority (Priority Three) requests, 6.27

Medium priority (Priority Two) requests, 6.28

Software access for customers or employees, provisions for, 6.4, 6.23

Teeth of SLA, 6.24-6.25

Termination of, 6.24-6.25

Uptime guarantee, 6.24-6.25

Warranties compared, 6.10, 6.17

Service Marks. See Trademarks, Service Marks, and Trade Names

Service Providers. See Internet Service Providers (ISPs)

Setoffs

Software licensee's waiver of setoff rights in bankruptcy proceedings, 12.12

Sexually Oriented Materials

See also **Obscenity; Pornography**

CAN-SPAM Act, applicability of, 17.18, 17.20, 17.22

Shares and Shareholders

Common stock, 16.2, 16.5

Drag-along rights, 16.10

Equity financing. See **Equity Financing**

Preferred stock. See **Venture Capital Financing**

Shopping Cart Programs

Generally, 10.12

Evaluation of, 10.13

Exclusive licensing of shopping cart technology, 5.19

Warranty against infringement of licensing, 6.10

Shrink-Wrap License Agreements

Defined, 7.1

Enforceability of, 7.2

Installation and use of software signaling agreement by customer, 7.2

Nonexclusive license, shrink-wrap agreement as, 12.3

Uniform Computer Transactions Act (UCITA), effect of, 7.11

Signatures

Electronic Signatures in Global and National Commerce Act (E-Sign). See **E-Sign**

Promissory notes, signature requirements, 16.25

Slander. See Defamation

SLAPP Statute. See Anti-SLAPP Statute

Small Business Administration (SBA)

Loans and loan guaranties by SBA, 16.15

Software

Copyright registration, depositing requirements for computer program, 1.8A

Electronic data discovery (EDD) software, 20A.32, 20A.34

Encryption software. See **Encryption Software**

Export controls. See **Export Controls on Commercial Software and Technology**

Filtering software. See **Filtering Software**

Hosting agreement, responsibility for customers' or employees' software access, 6.4, 6.6

Patents. See **Patents**

Publicly available software defined, 21.29

Secure transaction processing software. See **Secure Transaction Processing Software**

Service level agreements (SLAs), provisions for software access for customers or employees, 6.4, 6.23

Technical support. See **Technical Support**

Trade dress protection for, 3.78

Trade secret protection for software, 2.22

User interface of software programs, trade dress protection for, 3.78

Software Developers

Evaluation of software

Generally, 13.4

Sample form, software test and evaluation agreement, 13.5

Freeware. See **Open Source Software**

General technology companies offering custom software development services, 5.10

License agreements. See **Software License Agreements**

Open source software. See **Open Source Software**

Software development agreement

Generally, 13.1

Ownership rules, 13.2

Sample form, 13.3

Websites. See **Website Development**

Software License Agreements

Generally, 12.1

American Law Institute (ALI) software contract principles, 7.12

Assignment of, 12.12

Bankruptcy laws, impact of

Generally, 12.11

Drafting considerations, 12.13

Executory contracts and Bankruptcy Code §365(n), 12.12-12.13

Beta user evaluation agreement, 8.6, 8.7

Breach of contract, rejection of software license constituting, 12.12

Browse-wrap agreement, modification of software license through, 7.4

Canned software, 10.25

Choice of law or choice of forum provisions in, 8.4

Click-wrap agreements. See **Click-Wrap Agreements**

Consideration for, 12.2, 12.5

Custom software, 10.25

Damages

Limitation or exclusion of damages provisions in, 8.4

Liquidated damages clause, 12.13

End-user license agreements (EULAs)

Click-wrap agreements. See **Click-Wrap Agreements**

Form, 8.5

Shrink-wrap license agreement. See **Shrink-Wrap License Agreements**

Exclusive licenses

Generally, 12.2, 12.7

Exclusivity clause, 12.10

Performance milestones, 12.2, 12.9

Restrictions on scope or field of use, 12.8

Royalties, 12.9

Executory contracts, software licenses as, 12.12-12.13

Fees (see License fees, below)

Form of agreement, 12.6, 12.7

Hosting agreements. See **Hosting Agreements**

Independent contractors, 4.18

License fees

Online agreement, fee provisions in, 8.4

Payment of, 6.40, 12.5

Reduction of fees if future improvements no longer provided, 12.13

Royalties (see Royalties, below)

Nonexclusive licenses, 12.3-12.4A, 12.7

Number of end users, 12.4A

Online agreements

Generally, 8.1, 8.4

Beta user evaluation agreement, 8.6, 8.7

End-user software license agreement, 8.5

Evaluation license agreement, 8.10, 8.11

Limits on licensee's use and scope, 8.4

Open source software license agreement, 8.8, 8.9

Toolkit license agreement for software developers, 8.12, 8.13

Open source software license agreement, 8.8, 8.9

Payment structures, 12.5

Royalties

Calculation of royalty base, 12.5

Exclusive license, effect of, 12.2, 12.9

Minimum guaranteed annual royalty, 12.9

Modification, copy, and distribution rights, royalty for, 12.4

Percentage of licensee's gross or net revenues, royalty as, 12.5

Rejection of license in bankruptcy proceedings, effect of, 12.13

Reporting requirements, 12.12

Sublicensing rights, effect of, 12.7

Sales and use taxes, applicability of, 10.25

Scope of license, 8.4, 12.4, 12.7-12.8

Shrink-wrap license agreements. See **Shrink-Wrap License Agreements**

Source code escrow agreement, use of, 12.7, 12.13

Sublicensing rights, 12.7

Termination of, 12.12-12.13

Trade secret information, confidentiality provision protecting, 8.4

Warranty provisions, 8.4, 12.7, 12.12

Source Code Escrow

See also **Coding**

Agreement, sample form, 15.2

Purpose of source code escrow services, 15.1

Software license agreement, source code escrow agreement supplementing, 12.7, 12.13

Spam E-Mail

Generally, 17.11

Anti-spam litigation, 17.28

Blocking spam, practical methods, 17.29

CAN-SPAM Act. See **CAN-SPAM Act**

Click-wrap agreement prohibiting e-mail users from distributing spam, 7.3

Computer Fraud and Abuse Act, applicability of, 18.3-18.4

Costs

Generally, 17.11

California's anti-spam law, recovery of costs under, 17.25

Defined, 17.1

First Amendment, applicability to spam e-mail, 17.11, 20.24

Spoofing, 17.19, 17.28

State anti-spam laws

Generally, 17.24

California anti-spam laws, 17.25-17.26

Penal Code §502, 17.27, 18.16

Preemption of state law by CAN-SPAM Act, 17.12, 17.25-17.26

Trespass to chattels, 17.28, 18.20

Spoliation of Evidence. See Evidence

Spoofing, 17.19, 17.28

Spyware

Generally, 9.6B

Consumer Protection Against Spyware Act, prohibitions under, 9.26A

Statutes of Limitations

See also **Time**

No Electronic Theft Law (NET Act), extending criminal statute of limitations for copyright infringement under, 8.26

Stored Communications Act, 18.8, 18.11

Strategic Alliances

Agreement for strategic alliance, sample form, 11.4, 11.5

Co-branding. See **Co-Branding**

Defining term, 11.1

Intent re strategic alliance, sample letter, 11.3

Key structuring issues, 11.2

Types of alliances, 11.2

Streaming Audio and Video

Music on Internet, 8.22, 8.27

Obtaining licenses from intellectual property owners before launch of website, 14.15, 14.16

Streamlined Sales Tax Agreement, 10.20A

Strike, Motion to

California Anti-SLAPP statute, motion to strike complaint under, 20.25

Subpoenas

Digital Millennium Copyright Act (DMCA), copyright owners subpoenaing names of alleged infringers from ISPs, 1.29, 1.41

Electronically stored information (ESI), subpoenas for. See **Electronically Stored Information (ESI), Discovery of**

Right to Financial Privacy Act (California and Federal), disclosure in response to subpoena or search warrant, 9.13, 9.23

Subsidiaries

Exporting encrypted software to U.S. subsidiaries, regulations affecting, 21.39

Tables. See Charts, Checklists, Questionnaires, and Tables

Tangible Property

Insurance coverage. See **Insurance for On-Line Businesses**

Trade secrets not qualifying as, 20.36

Taxes (Generally)

Lease financings of equipment, tax advantages of, 16.16

Sales and use taxes. See **Sales and Use Taxes**

Tax on Internet transactions. See **Tax on Internet Transactions**

Tax on Internet Transactions

California tax policy, 10.21

Formulation of e-commerce tax policy, 10.17

International e-commerce tax policy, 10.18

Internet Tax Freedom Act (ITFA), 10.17-10.18, 10.20

Sales and use taxes. See **Sales and Use Taxes**

Shopping cart service, automatic tax and shipping calculations by, 10.13

Streamlined Sales Tax Agreement, 10.20A

United States federal tax policy

Internet Tax Freedom Act, 10.17-10.18, 10.20

Treasury Department, role of, 10.19

Value Added Taxes (VAT), EU requiring non-EU vendors of digital products to charge on Internet sales to EU consumers, 21.16

Technical Support

Generally, 6.40

Basic technical support exhibit, 6.48, 6.49

Form of technical support and maintenance agreement, 6.45, 6.46

Frequently Asked Questions (FAQs) documentation, 6.47

General technology companies, technical support provided by, 5.10

Help desk, 6.44

Providing technical support to customers, 6.47

Reporting requirements, 6.43

Response times, 6.43, 6.45

Software support and maintenance agreements, generally, 6.41, 10.25

Support services, 6.43

Training, 6.44, 6.47

Upgrades and maintenance fees, 6.42-6.43, 6.45

Telephone Sales

FTC's Mail or Telephone Order Merchandise Rule, compliance with, 10.16

Governing law, 17.8, 17.10

Order processing, 10.10

Tenants in Common

Co-owners of copyright treated as tenants in common, 1.4

Terms of Use

Generally, 8.2

Computer Fraud and Abuse Act, applicability to conduct exceeding terms of use, 18.5

Defined, 8.1

Websites

End user payment terms, 10.14, 10.15

Form of website terms of use, 8.3

Terrorism

Export controls. See **Export Controls on Commercial Software and Technology**

USA Patriot Act cyberterrorism provisions, 18.12

Third Parties

Banner advertisements on third party's website, 17.1

Copyrights. See **Copyrights**

Domain names. See **Domain Names**

Electronic data discovery, use of third-party data-hosting service for, 20A.47

Export control laws, third party vendors and customers' agreement to not export or reexport software in violation of, 21.56

Federal Trade Commission Act, third party's liability for deceptive advertising under, 17.4

Lanham Act, using third party's trademark as metatag as violation of, 3.71

License grant allowing third party to host or maintain website, 5.17

Trademarks, third party's concurrent use of. See **Trademarks, Service Marks, and Trade Names**

Website developer, indemnification agreement covering claims for infringement of patents, copyrights, and third party intellectual property rights, 3.78

Time

See also **Statutes of Limitations**

Copyright protection, duration of, 1.3

Copyright registration, time considerations, 1.8B

Credit card transactions, time for settlement of, 10.3

Debit card transactions, transfer of funds through, 10.4

Domain name infringement claim, time limit for appealing arbitration panel's decision, 3.21

Extension of time. See **Extension of Time**

FTC's Mail or Telephone Order Merchandise Rule, timely shipment under, 10.16

Hosting agreements, provisions for deadlines and turnaround times in, 6.9

Internet advertising agreement, termination clause within, 17.34

Internet checks, processing time for, 10.5

Internet Tax Freedom Act (ITFA), 3-year moratorium on imposition of new taxes on Internet access under, 10.20

Opt-out requests for spam e-mail, time considerations, 17.16

Patents, term of, 2.4

Service level agreements. See **Service Level Agreements (SLAs)**

Trademark, duration of registered, 3.52

Trade secret, unlimited duration of, 2.4, 2.22

Website, drafting timetable for delivery of, 5.14-5.16

Toolkits

Online software developer toolkit license agreement, 8.12, 8.13

Tracking Software

See also **Privacy**

Adware. See **Adware**

California constitutional claims of violation of privacy, 9.16

Computer Fraud and Abuse Act, applicability of, 18.6

Data mining of customer information, 9.6

Electronic Communications Privacy Act, applicability of, 18.6, 18.10

Spyware. See **Spyware**

Trade Dress

Generally, 3.77

Infringement of trade dress

Generally, 3.79

Burden of proof on plaintiff in action for infringement of unregistered trade dress, 3.77

Inherent distinctiveness or secondary meaning (see Inherent distinctiveness or secondary meaning of trade dress as element of infringement, below)

Likelihood of confusion, effect of, 3.87

Nonfunctionality (see Nonfunctionality of trade dress as element of infringement, below)

Inherent distinctiveness or secondary meaning of trade dress as element of infringement

Generally, 3.84

Product designs, secondary meaning required for protection of, 3.85

Product packaging, inherent distinctiveness of, 3.85

Website user interfaces as product packaging or product design trade dress, 3.86

Nonfunctionality of trade dress as element of infringement

Generally, 3.80

Aesthetic functionality, doctorate of, 3.82

Four-factor test to determine if trade dress functional, 3.81

Patent protection distinguished, 3.80

Secondary meaning of trade dress (see Inherent distinctiveness or secondary meaning of trade dress as element of infringement, above)

Software, protection for, 3.78

Types of trade dress, 3.77

Website user interface, protection for

Generally, 3.78

Functionality of website user interfaces, effect on trade dress protection, 3.83

Product design or product packaging trade dress, website user interfaces as, 3.86

Trademark Act of 1946. See Lanham Act

Trademarks, Service Marks, and Trade Names

Generally, 3.26

Abandonment of trademark

Generally, 3.53

Defense to infringement action, abandonment of trademark as, 3.64

Amendments

Abandonment of trademark, amendment of trademark resulting in, 3.53

Application for registration, restrictions on amending drawing of trademark included in, 3.43

Changing or amending mark, effect of, 3.53

Anti-Phishing Act of 2005, effect of, 3.63, 9.6C

Assignment of trademarks

Generally, 3.57, 16.29-16.30

Form of trademark assignment, 3.58

Goodwill of business, assignment of trademark invalid without accompanying assignment of, 3.57, 5.1, 16.29

Invalidity of assignments in gross, 3.57

Pending trademark application, assignment of, 3.57

U.S. Patent and Trademark Office Cover Sheet, 3.59

Attorney fees in infringement action, recovery of, 3.30, 3.63

California anti-cybersquatting statute, inapplicability to trademarks, 20.32

Characterization of marks, 3.28

Concurrent use of mark by third party

Concurrent use application, 3.40

Contents of application for registration, identifying concurrent use of mark in, 3.38

Contents of application

Generally, 3.38

Bases for filing, application for registration specifying, 3.42

Concurrent use of mark (see Concurrent use of mark by third party, above)

Description of graphic mark, 3.44

Drawing of mark, inclusion with original application, 3.43

Goods and services used in connection with mark, identification and classification of, 3.41

Information about applicant, inclusion of, 3.39

Verified statement of facts, inclusion of, 3.40

Damages, recovery in infringement action

Generally, 3.63

Treble damages, recovery of, 3.30

Defenses

Anti-dilution claims, defenses to, 3.68

Fair use as defense to allegations of trademark infringement, 3.64, 3.72

Infringement claims, defenses to, 3.64, 3.72

Dilution of famous mark

Generally, 3.65

Commerce, requirement that infringing mark be used in, 3.67

Complaint site, dilution claim against, 20.29

Cybersquatters, anti-dilution claim against, 3.67

Factors in determining if mark famous, 3.66

Remedies and defenses to anti-dilution claims, 3.65, 3.68

Duration of registered mark, 3.52

Employees, policies prescribing allowable uses of trademarks by, 3.53

Evidence. See **Evidence**

Fair use

Generally, 3.68

Defense to infringement claim, fair use of trademark as, 3.64, 3.72

Nominative fair use, 3.72

Famous names of politicians, athletes, and celebrities, trademark protection for, 20.30

Fees for registration

Generally, 3.41

Opposition to registration, filing fee for, 3.49

Renewal of registration, fee for, 3.52

Geographically deceptively misdescriptive mark, three-part test to determine, 3.32

Geographic regions, right to use mark limited to specific, 3.29

Goodwill

Assignment of trademark invalid without accompanying assignment of goodwill of business, 3.57, 5.1, 16.29

Metatag, misspelling of trademark constituting misappropriation of competitor's goodwill, 3.75

Grant or denial of registration

Appeal from denial of registration, 3.50

Cancellation proceedings, 3.49

Opposition to registration, filing of, 3.49

Incontestability of mark after 5 years of continuous use in commerce, 3.30

Infringement of trademark

Generally, 3.60

Anti-Phishing Act of 2005, effect of, 3.63, 9.6C

Attorney fees, recovery of, 3.30, 3.63

Burden of proof, 3.60

Cease and desist letter, 3.69, 3.70

Complaint site, infringement claim against, 3.64, 20.29

Damages (see Damages, recovery in infringement action, above)

Defenses to trademark infringement, 3.64, 3.72

Fair use (see Fair use, above)

Insurance coverage for infringement claim, 20.39

Likelihood of confusion, factors in determining, 3.60, 3.87, 20.29

Metatags. See **Metatags**

Injunctive relief

Generally, 3.63

Dilution of mark, injunction against, 3.65, 3.68

Similar marks, senior user's injunction against junior users from using, 3.29

Licensing of trademark

Generally, 3.54

Abandonment of trademark as result of not restricting licensee's use of licensed mark, 3.53

Agreement for licensing trademark, 3.56

Guidelines for trademarks, 3.55

Naked license defined, 3.53

Likelihood of confusion

Generally, 3.60, 3.87, 20.29

Metatags, applicability of likelihood of confusion test to use of third party trademarks as, 3.71

Linking arrangements, trademark issues associated with, 8.16

Metatags. See **Metatags**

Priority of use, trademark rights based on, 3.29

Registration

Generally, 5.1

Acceptance of application, assignment of serial number to identify mark, 3.37

Coined, arbitrary, fanciful, or suggestive marks, registration of, 3.28

Contents of application (see Contents of application, above)

Descriptive marks, requirements for registration of, 3.28-3.29

Distinctiveness of mark, requirement for registration, 3.28

Domain names, registration as trademarks. See **Domain Names**

Federal registration, benefits of, 3.30

Filing fees (see Fees for registration, above)

Foreign language, grounds for rejecting mark in, 3.45

Form of application, 3.36

Grant or denial of registration (see Grant or denial of registration, above)

Improper use of trademark symbol before registration, consequences of, 3.51

Intent-to-use application, 3.35, 3.42

Madrid Protocol, obtaining trademark protection in foreign countries under, 3.48

Mere description of goods and services associate with mark, nonregistrability of, 3.28

Prerequisites for registration on principal register, 3.34

Principal register, registration of marks on, 3.28, 3.34

Renewal of registration, 3.52

Restrictions on registration of trade names under federal law, 3.27

Review of application by examining officer, 3.37

Searching for same or similar trademarks prior to registration, 3.33

Secondary meaning as prerequisite for registration of nondistinctive trademark, 3.34

State law, trademark rights under, 3.31

State level, registration of mark at, 3.26

Statutory basis for refusing to register trademark, 3.34

Supplemental register, registration of marks on, 3.28, 3.34, 3.49

Trade name, restrictions on registration as trademark, 3.47

Unregistered trademarks (see Unregistered trademarks, below)

Unregistrable trademarks, 3.32

Validity of trademark, effect of failure to register on, 3.26

Rights involving trademarks, preservation of, 3.53

Search engines

Trademark Electronic Search System (TESS), searching for federally registered trademarks in, 1.40

Unregistered trademarks and business names, using search engines to locate, 3.5

Security interests in trademarks, perfecting, 16.29

Symbol denoting trademark, use of, 3.51

Third parties

Concurrent use of mark by third party (see Concurrent use of mark by third party, above)

Domain names infringing on third party's trademark. See **Domain Names**

Metatags, applicability of likelihood of confusion test to use of third party trademarks as, 3.71

Trade dress. See **Trade Dress**

Trademark Act of 1946 (Lanham Act), 3.26

Trademark Electronic Search System (TESS), searching for federally registered trademarks in, 3.5

Unregistered trademarks

Common law protection for, 3.31

Searching for unregistered trademarks, 3.5

Violation of trademark rights

Anticybersquatting Consumer Protection Act (ACPA), protection for marks under, 3.62

Dilution of famous mark (see Dilution of famous mark, above)

False designation of origin, false description, or false and misleading representation of fact in connection with goods or services, 3.61

Infringement of trademark (see Infringement of trademark, above)

Palming off and reverse palming off defined, 3.61

Websites, including company trademarks on, 5.17

World Intellectual Property Organization (WIPO), alternative dispute resolution services offered by, 21.9

Trade Secrets

Generally, 2.20

Computer source and object code, 2.22A

Copyrightable trade secrets, 16.31

Customer lists, trade secret protection for, 2.22-2.23

Definition of trade secret, 2.21, 2.38

Disclosure of trade secrets, protection against (see Protection of trade secrets, below)

Examples of trade secrets, 2.22

Misappropriation of trade secrets

Damages or reasonable royalty for trade secret, plaintiff's election to receive, 2.36

Defenses to misappropriation claim, 2.35

Economic Espionage Act of 1996, criminal and monetary penalties for misappropriation, 2.38

Litigation, asserting trade secret privilege during, 2.37

Punitive damages for, 2.36

Uniform Trade Secrets Act, asserting misappropriation claim under, 2.34

Patent, trade secret protection as alternative to, 2.4

Perfecting security interest in trade secrets, 16.31

Protection of trade secrets

Generally, 2.25

Company policy on trade secret protection, 2.30, 2.31

Confidentiality agreements. See **Confidentiality and Invention Assignment Agreements**

Departing employees, stressing importance of trade secrets to, 2.26

Encryption of information transmitted on Internet to prevent access to trade secrets, 2.27

Firewalls within and between networks to protect trade secrets, 2.27

Inevitable disclosure doctrine, effect of, 2.26

Injunction to protect trade secrets, 2.26, 2.34

Loss of trade secret protection, 2.24

Marking trade secret documents as confidential, 2.29

Nondisclosure agreement between company and individual with access to trade secrets, 2.25, 2.32, 2.33, 2.37

Physical security of company's facilities, 2.28

Review of website contents to protect trade secrets, 14.4

Software license agreements, protection of trade secret information through confidentiality provision, 8.4

State law, trade secrets protected under, 2.20

Website development, protecting against unintended release of trade secret information during, 5.20

Recipes and manufacturing processes, 2.22B

Reverse engineering. See **Reverse Engineering**

Security agreement and financing statement prohibited from jeopardizing confidentiality by describing, 16.31

Software, trade secret protection for, 2.22

Statutory definition of trade secret, 2.21, 2.38

Tangible property, trade secrets not qualifying as, 20.36

Unlimited duration of trade secret, 2.4, 2.22

Transfer of Property

See also **Assignment**

Copyrights, transfers of. See **Copyrights**

Domain name, transfer of. See **Domain Names**

Intellectual property, agreement for transfer and assignment of, 5.3

Patents, transfer of. See **Patents**

Treaties

Patents, treaties concerning, 2.14

Treble Damages. See Damages

Trespass to Chattels

Generally, 18.17

Class action complaint, 18.20A

Computer hacking, applicability of trespass to chattels doctrine to, 18.21A

Linking arrangements, potential liability for trespass to chattels with, 8.17

Physical harm to chattel as basic element of tort, 18.21

Spam e-mail constituting trespass to chattels, 17.28, 18.20

Trojan Horse, 18.1

UBE. See Spam E-Mail

UCC. See Uniform Commercial Code (UCC)

UCITA. See Uniform Computer Transactions Act (UCITA)

UETA. See Uniform Electronic Transactions Act (UETA)

Unfair Competition

Communications Decency Act (CDA), defense against claim of unfair competition, 20.7

Misrepresentation of company privacy or data mining practices, remedies for, 9.27

Unfair or Deceptive Trade Practices

Liability for company's failure to adhere to privacy policy or to disclose data mining of customer information, 9.9

Uniform Commercial Code (UCC)

Definition of signed under UCC, 7.5

Domain names as general intangibles under UCC, 16.30

Filing UCC-1 financing statements to perfect security interests in intellectual property collateral, 16.21, 16.26-16.31

Lanham Act, no preemption of UCC by, 16.29

Trade secrets as general intangibles under UCC, 16.31

Uniform Computer Transactions Act (UCITA)

Generally, 7.11

Bomb-shelter (anti-UCITA) legislation protecting software licensees from UCITA choice-of-law provisions, 7.11

Prominent display of non-interactive terms on website under, 7.4, 7.11

Uniform Domain Name Dispute Resolution Policy (UDRP). See Domain Names

Uniform Electronic Transactions Act (UETA)

Generally, 7.9

Consent under UETA, 7.10

E-Sign. See **E-Sign**

Uniform Resource Locator (URL), 3.1

Unsolicited E-Mail. See Spam E-Mail

Uploading Content. See Downloading and Uploading Content

URL. See Uniform Resource Locator (URL)

USA Patriot Act

Cyberterrorism, deterrence and prevention of, 18.12

Usury

Debt financing, usury issues for nonbank lenders, 16.22

Exemptions, 16.22

Utility Patents. See Patents

Valuation

Enterprise value of company, determining, 5.1

Equity financing, valuation of company for purposes of, 16.5, 16.8

Fair use, effect on potential market or value of copyrighted work, 1.22

Value Added Taxes (VAT)

EU requiring non-EU vendors of digital products to charge on Internet sales to EU consumers, 21.16

Vendors

Out-of-state vendors, laws regulating sales by, 17.10

Software developers. See **Software Developers**

Technical support. See **Technical Support**

Third-party vendors providing support and maintenance services when software license rejected in bankruptcy proceedings, 12.13

Venture Capital Financing

Generally, 16.7

Bridge loan, 16.3, 16.7, 16.34

Ownership, dilution of, 16.7, 16.10

Preferred stock financing

Generally, 16.2, 16.7

Term sheet for preferred stock financing, 16.8-16.9, 16.10

Strategic partners, 16.7

Structure of venture capital financings, 16.8

Venue

See also **Jurisdiction**

Click-wrap agreements to avoid venue disputes, 7.3

Dismissal for commencing action in forum other than one specified in contractual choice-of-forum clause, 19.12

Vesting

Venture capital financing agreements including vesting agreement, 16.8

Vicarious Liability

Communications Decency Act (CDA), Internet service provider's immunity from vicarious liability for defamatory statements made by subscribers, 20.1

Videos

Streaming video license. See **Streaming Audio and Video**

Testimonials, sample endorsement agreement, 14.9, 14.10

Video rental records, online data mining of customer information, 9.8

Viruses

See also **Cyberattacks**

Generally, 18.1

Electronically stored information (ESI), risk of virus infection during collection of, 20A.35

Terms of use policies regarding upload of viruses, 8.3

Warranty in hosting agreement providing that servers and software free from viruses and harmful code, 6.10

Worms, 18.1

Waiver

Attorney-client privilege, waiver of, 20A.7

Loan agreement, waiver of reporting provisions in, 16.24

Software licensee's waiver of setoff rights in bankruptcy proceedings, 12.12

Work product privilege, waiver of, 20A.7

Warranties. See Representations and Warranties

Warrants

Stock option, 16.2

Web Bugs

Generally, 9.5

California constitutional claims of violation of privacy, 9.16

Data mining of customer information, 9.5

Web Portals. See Hosting Agreements

Website Development

Generally, 5.4

Agreements

Drafting (see Drafting website development agreement, below)

Form of website development agreement, 5.24, 5.25

Independent contractor agreements, contents of, 5.23

Content of website, responsibility for, 5.15

Developers

Generally, 5.7

General technology companies, 5.10

Independent contractors. See **Independent Contractors**

Ongoing obligations of developer, 5.22

Website development specialists, 5.9

Drafting website development agreement

Generally, 5.14

Attorney's role, 5.1, 5.5-5.6

Confidentiality provisions, 5.20, 5.26

Deliverables and timelines for delivery, 5.14-5.16

Ethical considerations, 5.5

Functional specifications for website features, 5.15-5.16

Ownership issues (see Ownership issues, below)

Parties' responsibilities, 5.15

Representations and warranties of developer, 5.21-5.22

Upgrading website, 5.21-5.22, 5.26

E-Commerce Transactions. See **E-Commerce Transactions and Payments**

Hosting services provided by website development specialists, 5.9

Independent contractors, use of. See **Independent Contractors**

Modification of company-furnished content by website developer, 5.17, 5.26

Ownership issues

Generally, 5.1

Conflicting ownership interests, 5.11

Domain name registration, 5.13

Grants of ownership and license rights, 5.17-5.20

Shelf code used by developer, effect on allocation of ownership rights, 5.15, 5.18-5.19

Work made for hire, website exempt from doctrine of, 5.12

Timetables for delivery of website, 5.14-5.16

Upgrading website, 5.21-5.22, 5.26

Websites (Generally)

Advertising. See **Advertising**

Bulletin boards. See **Bulletin Boards**

California Department of Consumer Affairs (DCA), 17.9, 17.29

California State Board of Equalization (BOE), list of taxable transactions, 10.24

Complaint sites. See **Complaint Sites**

Contents of website. See **Content of Website, Obtaining Licenses and Rights to Use**

Copyright protection for, 1.2

Creative Commons, 14.18

Development of. See **Website Development**

Domain names. See **Domain Names**

Dot Com Disclosures, FTC guidelines, 17.5

Electronic Frontier Foundation, 8.28

Free Software Foundation, 8.8

FTC. See **Federal Trade Commission (FTC)**

Hacking Lexicon, 18.1

Hosting agreements. See **Hosting Agreements**

Identify theft, Office of Privacy Protection, 9.3

Identity theft, website for combating, 9.2

Indemnification agreement with website developer covering claims for infringement of patents, copyrights, and third party intellectual property rights, 3.78

Kidz Privacy, 9.36

Metatags. See **Metatags**

Open Source Initiative, 8.8

Privacy policies for websites. See **Privacy**

Small Business Administration (SBA), 16.15

Streamlined Sales Tax Project, 10.17

Terms of use. See **Terms of Use**

Trade dress protection for website user interface. See **Trade Dress**

Uniform Electronic Transactions Act (UETA) fact sheets, 7.9

US-CERT (Computer Emergency Readiness Team), 18.22

U.S. Department of Justice, Computer Crime and Intellectual Property Section of Criminal Division, 18.2, 18.14

Watchdogs, 9.42

Wikipedia, 14.18

World Intellectual Property Organization (WIPO), website for, 2.14

World Trade Organization (WTO), 10.18

Wireless Networks and Devices

Business and Professions Code §22948.6, requirements for wireless devices under, 18.16A

CAN-SPAM Act, applicability to commercial e-mails sent to wireless devices, 17.23A

Computer Fraud and Abuse Act (CFAA), applicability to wireless networks, 18.7A

Electronic Communications Privacy Act (ECPA), applicability to unauthorized wireless access, 18.11A

Miscellaneous wireless encryption items, 21.34B

Pen Register Act, applicability of, 18.11A

Wiretap Act, 9.15, 18.8

Words and Phrases. See Construction and Interpretation; Definitions

Work Made for Hire

Copyrights. See **Copyrights**

Defined, 1.5

Independent contractors. See **Independent Contractors**

Work Product Privilege

Fed R Evid 502, 20A.44A

Waiver of, 20A.7

World Intellectual Property Organization (WIPO)

Generally, 21.9

Alternate dispute resolution

Generally, 21.9

Proposal for, 21.20

Selection of arbitrator, 3.14

Madrid Protocol, 3.48

Uniform Domain Name Dispute Resolution Policy (UDRP)

Complaint, 3.17, 3.18

Response, 3.19, 3.20

Website for, 2.14

World Trade Organization (WTO)

International e-commerce tax policy addressed by WTO, 10.18

Worms, 18.1

Writings

Copyright, writing required for transfer of, 1.9

Hosting agreements. See **Hosting Agreements**

Intellectual property, written assignment of, 5.1

Software licensee's request that licensor continue to perform obligations under license, 12.12

Trademark, requirement of written instrument for assignment of, 3.57

Website development agreements. See **Website Development**

WTO. See World Trade Organization (WTO)

© The Regents of the University of California