



1 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Publication Information

1 MB Practice Guide: CA E-Discovery and Evidence Author(s)

Author(s)

Matthew Bender[(R)] Practice Guide: California E-Discovery and Evidence
Michael F. Kelleher
Editorial Consultant

For easy access to this publication online,
See <http://www.lexisnexis.com/MBPracticeGuide/CA>
2010



2 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Publication Information

1 MB Practice Guide: CA E-Discovery and Evidence Questions?

Questions?

Technical Questions?

Phone: (800) 223-5297
Fax: (800) 533-1645 or (518) 487-3191
E-Mail: technical.support@lexisnexis.com
Visit Our Web Site: <http://www.lexis.com>

Editorial Questions?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call: West
Paul F. Getchell, J.D. Paul.F.Getchell@lexisnexis.com at 1-800-424-0651 (ext. 3234)
James T. Hardin, J.D. James.Hardin@lexisnexis.com at 1-800-424-0651 (ext. 3339)
Outside the United States and Canada, please call (973) 820-2000
For assistance with replacement pages, shipments, billing or other customer service matters, please call:
Customer Services Department at (800) 833-9844
Outside the United States and Canada, please call (518) 487-3000
Fax Number (518) 487-3584
Customer Service Website <http://www.lexisnexis.com/custserv/>
For information on other Matthew Bender publications, please call
Your account manager or (800) 223-1940
Outside the United States and Canada, please call (518) 487-3000



3 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Publication Information

1 MB Practice Guide: CA E-Discovery and Evidence Cite As

Cite As

Cite as:

Kelleher, Matthew Bender(R) Practice Guide: Cal. E-Discovery and Evidence, §



4 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Publication Information

1 MB Practice Guide: CA E-Discovery and Evidence Copyright

Copyright

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

LexisNexis and the Knowledge Burst logo are registered trademarks and Michie is a trademark of Reed Elsevier Properties Inc., used under license. Matthew Bender and the Matthew Bender Flame Design are registered trademarks of Matthew Bender Properties Inc.

Copyright © 2010 Matthew Bender & Company, Inc., a member of the LexisNexis Group.
All Rights Reserved.

No copyright is claimed in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material exceeding fair use, 17 U.S.C. § 107, may be licensed for a fee of 25cent(s) per page per copy from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.



5 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Publication Information

1 MB Practice Guide: CA E-Discovery and Evidence Statement on Fair Use

Statement on Fair Use

RELEASE NO. 3, AUGUST 2010

LexisNexis Matthew Bender recognizes the balance that must be achieved between the operation of the fair use doctrine, whose basis is to avoid the rigid application of the copyright statute, and the protection of the creative rights and economic interests of authors, publishers and other copyright holders.

We are also aware of the countervailing forces that exist between the ever greater technological advances for making both print and electronic copies and the reduction in the value of copyrighted works that must result from a consistent and pervasive reliance on these new copying technologies. It is LexisNexis Matthew Bender's position that if the "progress of science and useful arts" is promoted by granting copyright protection to authors, such progress may well be impeded if copyright protection is diminished in the name of fair use. (See Nimmer on Copyright § 13.05[E][1].) This holds true whether the parameters of the fair use doctrine are considered in either the print or the electronic environment as it is the integrity of the copyright that is at issue, not the media under which the protected work may become available. Therefore, the fair use guidelines we propose apply equally to our print and electronic information, and apply, within §§ 107 and 108 of the Copyright Act, regardless of the professional status of the user.

Our draft guidelines would allow for the copying of limited materials, which would include synopses and tables of contents, primary source and government materials that may have a minimal amount of editorial enhancements, individual forms to aid in the drafting of applications and pleadings, and miscellaneous pages from any of our newsletters, treatises and practice guides. This copying would be permitted provided it is performed for internal use and solely for the purpose of facilitating individual research or for creating documents produced in the course of the user's professional practice, and the original from which the copy is made has been purchased or licensed as part of the user's existing in-house collection.

LexisNexis Matthew Bender fully supports educational awareness programs designed to increase the public's recognition of its fair use rights. We also support the operation of collective licensing organizations with regard to our print and electronic information.

No copyright is claimed in the text of statutes, regulation, and excerpts from court opinions quoted within this work.

Original Copyright::

(c) 2010 Matthew Bender & Company, Inc., a member of the LexisNexis Group. All rights reserved.

ISBN **978-1-4224-7110-4**

Library of Congress Card Number: 2009937910

MATTHEW BENDER & Co., INC.

Editorial Offices

121 Chanlon Rd., New Providence, NJ 07974 (908) 464-6800

201 Mission Street, San Francisco, CA 94105-1831 (415)908-3200



6 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Publication Information

1 MB Practice Guide: CA E-Discovery and Evidence Editorial Consultant

Editorial Consultant

Michael F. Kelleher

For over sixteen years, Michael F. Kelleher practiced complex commercial litigation in the San Francisco office of Folger Levin & Kahn LLP. Mr. Kelleher has a strong technical background in addition to his legal experience. In college he studied computer programming and did database work and synthesis in a graduate chemistry laboratory while earning his bachelor's degree in chemistry. Subsequently, he served as a naval officer on board a nuclear submarine, including service as Reactor Controls Officer and Communications Officer.

As a litigator, Mr. Kelleher frequently applied his engineering and science background to the litigation of electronic discovery issues. In 2003 and 2004, he had the opportunity to litigate electronic discovery issues extensively in the unfair competition case of PeopleSoft v. Oracle in Alameda County Superior Court. That case involved over 10 million pages of electronically stored information. In trade secret cases, he has also litigated spoliation claims and expert forensic recovery of deleted electronic data.

Mr. Kelleher is the general counsel of DS-IQ, Inc., a marketing technology company. Mr. Kelleher frequently writes and speaks on electronic discovery and litigation technology issues.

Mr. Kelleher is a graduate of the University of California, Berkeley School of Law (J.D., 1992, Order of the Coif) and the University of Utah (B.A. in chemistry, 1984, magna cum laude). After law school, he served as a law clerk to Judge Harold Fong, United States District Court for the District of Hawaii. Mr. Kelleher is a member of the California Bar, and is admitted to practice before the United States Patent and Trademark Office.



7 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Publication Information

1 MB Practice Guide: CA E-Discovery and Evidence Publisher's Editorial Staff

Publisher's Editorial Staff

Mark H. Wasserman, J.D.

Senior Director, Content Development

Paul F. Getchell, J.D.

Coordinating Editor

Jonathan E. Meyer, J.D.

Online Editor

Jeanne Fogler

Editor

Claudia Gurevich

Manager of Publishing Operations

Nehemias H. Salinas

Content Operations Analyst

Jay Huber

Index Manager

Pat Healy

Index Editor



8 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Publication Information

1 MB Practice Guide: CA E-Discovery and Evidence Contributing Authors and Editors

Contributing Authors and Editors

Scott Andre, Esq.

Diane E. Barry, Esq.

Edward L. Baskauskas, Esq.

Jill Brown, Esq.

Janet C. Graham, Esq.

Ernst Halperin, Esq.

Fay Hulett-Nelson, Esq.

Nicole Johnson, Esq.

Lisa Leighton, Esq.

Helen L. Marsh, Esq.

Jennifer Ross, Esq.

Steven N. Williams, Esq.



9 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Publication Information

1 MB Practice Guide: CA E-Discovery and Evidence Abbreviations

Abbreviations

United States Constitution and Statutory Sources

US Const United States Constitution

USC United States Code

USC app United States Code Appendices

IRC United States Code, Title 26 **California Constitution and Statutory Sources**

Cal Const California Constitution

B&P Code Business and Professions Code

CC Civil Code

CCP Code of Civil Procedure

Com Code Commercial Code

Corp Code Corporations Code

Ed Code Education Code

Elec Code Elections Code

Evid Code Evidence Code

Fam Code Family Code

Fin Code Financial Code

F&G Code Fish and Game Code

F&A Code Food and Agriculture Code

Gov Code Government Code

H&N Code Harbors and Navigation Code

H&S Code Health and Safety Code

Ins Code Insurance Code

Lab Code Labor Code

M&V Code Military and Veterans Code

Pen Code Penal Code

Prob Code Probate Code

PC Code Public Contract Code

PR Code Public Resources Code

PU Code Public Utilities Code

R&T Code Revenue and Taxation Code

S&H Code Streets and Highways Code

UI Code Unemployment Insurance Code

Veh Code Vehicle Code

Water Code Water Code

W&I Code Welfare and Institutions Code

Cal Stat California Statutes **California and Federal Regulations**

CCR California Regulations

CFR Code of Federal Regulations

Fed Reg Federal Register **California Attorney General Opinions**

Ops Cal Atty Gen Opinions of California Attorney General **Case Law**

US United States Supreme Court Reports

S Ct Supreme Court Reporter

L Ed Lawyer's Edition

L Ed2d Lawyer's Edition, Second Series

F Federal Reporter

F2d Federal Reporter, Second Series

F3d Federal Reporter, Third Series

F Supp Federal Supplement

F Supp2d Federal Supplement, Second Series

FRD Federal Rules Decisions

C California Reports

C2d California Reports, Second Series

C3d California Reports, Third Series

C4th California Reports, Fourth Series

CA California Appellate Reports

CA2d California Appellate Reports, Second Series

CA3d California Appellate Reports, Third Series

CA4th California Appellate Reports, Fourth Series

CA Supp California Appellate Reports, Supplement

CA2d Supp California Appellate Reports, Second Series, Supplement

CA3d Supp California Appellate Reports, Third Series, Supplement

CA4th Supp California Appellate Reports, Fourth Series, Supplement

CR California Reporter

CR2d California Reporter, Second Series

P Pacific Reporter

P2d Pacific Reporter, Second Series

P3d Pacific Reporter, Third Series **Federal Rules**

Fed R Civ P Rules of Civil Procedure

Fed R Civ P Appendix of Forms Rules of Civil Procedure, Forms Appendix

Fed R App P Federal Rules of Appellate Procedure

9th Cir R Circuit Rules

9th Cir R Appendix of Forms Circuit Rules, Forms Appendix

Sup Ct R Supreme Court Rules

Multidistrict R Multidistrict Rules

Fed R Evid Rules of Evidence

Fed R Bankr P Rules of Bankruptcy Procedure

Fed R Crim P Rules of Criminal Procedure **Central District abbreviations**

CD Cal Civ LR Local Rules

CD Cal Local Civil Appendix Civil Appendices

CD Cal Mag LR Magistrate Judge Rules

CD Cal Gen Order General Orders **Eastern District abbreviations**

ED Cal Gen LR General Rules

ED Cal Civ LR Civil Rules

ED Cal Mag LR Magistrate Judge Rules

ED Cal Automated Case Assignment Plan Automated Case Assignment Plan

ED Cal Gen Order General Orders **Northern District abbreviations**

ND Cal Civ LR Local Rules

ND Cal ADR LR Local Rules for Alternative Dispute Resolution

ND Cal Appendix Appendixes of Sample Forms

NC Cal Gen Order General Orders **Southern District abbreviations**

SD Cal Civ LR Local Rules

SD Cal Gen Order General Orders **California State Court Rules**

Cal Rules Ct California Rules of Court

Cal Rules Prof Conduct California Rules of Professional Conduct **Miscellaneous**

US Code Cong & Admin News Congressional and Administrative News

UST United States Treaties



10 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

What's New

1 MB Practice Guide: CA E-Discovery and Evidence Scope

Scope

HIGHLIGHTS

Release 3 August 2010

Admission of ESI

Ch. 15, covering the admission of electronically stored evidence, has been completely revised in this release.

Enhanced Glossary

New definitions have been added to the glossary in Ch. 1, Appendix A.

Social Networking

Coverage of social networking sites in the context of e-discovery has been added in this release.

2010 Midyear Update for Recent Judicial Decisions

The entire publication has been updated for recent California and federal judicial decisions. For a more detailed summary of the important changes incorporated into the publication in this release, see below.

This release contains the 2010 midyear update for Matthew Bender(R) Practice Guide: California E-Discovery and Evidence. Significant highlights of this release include the following:

Admission of Electronically Stored Information Into Evidence

Ch. 15, *Admissibility of Electronic Evidence at Trial*, has been completely revised in this release. The revised chapter deals with the issues that arise in getting ESI admitted into evidence in California litigation. Revision author Diane E. Barry, Esq., and practice consultant Hon. James L. Smith (Ret.) have focused on those aspects of the requirements for admission that present special issues when ESI is involved, including authentication, hearsay, and secondary evidence concerns. Each of these topics is explored in depth, with detailed discussion on the special issues that arise in the context of ESI and practical advice on how to resolve those issues. Two new forms have been added to the chapter: a stipulation regarding admission of items of ESI into evidence and a chain of custody record for ESI.

Expansion of Glossary

The glossary of terms in Appendix A of Ch. 1, *Understanding Electronic Information*, has been expanded to include new definitions, including revised definitions of Cache and Cookie, and new definitions of Decryption, Digital Signature, Encryption, Foreign Cookie/Third Party Cookie, Forensically Sound, FTP, Phishing, Public-Key Cryptography, Spoofing, and URL.

Social Networking Sites

Coverage of social networking sites in the context of electronically stored information has been expanded in this release. Discussion includes the nature and characteristics of such sites, their use in litigation, the effect of the Federal Stored Communications Act [see 18 U.S.C. § 2702(a)(2)] in the context of third party subpoenas to social networking sites, and ethical issues that may arise in accessing information posted on such sites. See Ch. 1, *Understanding Electronic Information*, 1.32[6]; Ch. 3, *Ethical Issues in E-Discovery*, 3.09[3]; and Ch. 6, *Demanding Production of Electronically Stored Information in California Court*, 6.17[6].

Recent Judicial Decisions

This release also adds coverage of California and federal decisions that have been compiled or become final since the cutoff date for Release 2. Significant new decisions include the following:

Discovery of Information on Web Hosting Sites. In *Zynga Game Networks, Inc. v. John Does 1-5* (ND CA, January 1, 2010) 2010 U.S. Dist. LEXIS 9390, *8 & *9, a social gaming company sued unknown defendants for infringing plaintiff's trademarks by selling online gaming chips that could be used in plaintiff's games. Plaintiff moved for an order permitting it to conduct discovery from four web hosting sites, ostensibly in order to discover the identities of the defendants, and seeking "all billing and account records (including all Internet domain names), server logs, website content, contact information, transaction histories and correspondence for the persons or entities that have purchased services ... in connection with the Internet domain name..." The court limited the scope of the proposed subpoenas to "all documents necessary to obtain the name, current and permanent addresses, telephone numbers, and valid e-mail addresses of the owner(s)" See Ch. 2, *Governing Law in E-Discovery*, 2.11[7].

Demanding Inspection of Computer/ Waiver of Privileged Communications. In *Dawe et al. v. Corrections USA et al.* (ED Cal 2009) 263 FRD 613, 619, the court granted defendants' motion to compel inspection of a third-party plaintiff's computer when (1) there was a high "level of contention and distrust that permeate[d] the litigation; (2) the third-party plaintiff had adamantly refused to permit "even a limited inspection of the computer"; and (3) there was evidence that another individual plaintiff's computer had been "forensically cleaned" prior to defendants' inspection. See Ch. 6, *Demanding Production of Electronically Stored Information in California Court*, 6.08[2]. In addition, attorneys for plaintiff produced a CD-ROM of e-mails without reviewing the e-mails. As a result, 227 attorney-client privileged e-mails were produced as part of a large electronic production that encompassed five thousand e-mail files. The court determined that, "on balance, and using a holistic reasonableness analysis, the plaintiff waived the privilege." See Ch. 8, *Responding to Electronic Discovery Demands in California Court*, 8.10[1].

Corporation Must Be In Good Standing To Assert Claims of Attorney-Client Privilege in E-Discovery. In *Software Rights Archive, LLC v. Google Inc.* (ND CA February 2010) 2010 U.S. Dist. LEXIS 11581, the court held that because claims of attorney-client privilege belong to the client, a client that is a corporation must be in good standing to successfully assert a claim of attorney-client privilege in an e-discovery response. See Ch. 8, *Responding to Electronic Discovery Demands in California Court*, 8.21.

Broad Discovery Available Under Federal Rules. In *Ferron v. Subscriberbase Holdings, Inc.* (SD Ohio Mar. 22, 2010) 2010 U.S. Dist. LEXIS 34414, a federal magistrate judge granted a motion by the defendants to compel the plaintiff to identify whether a certain internet protocol address was associated with his office email account. The court reasoned that the information was relevant to the question of whether the plaintiff, a lawyer by trade, was a "consumer" within the meaning of the Ohio Consumer Sales Practices Act under which he was suing the defendant for sending

allegedly misleading email solicitations. See *Ch. 9, Gathering and Producing Electronically Stored Information*, 9.05.

Meaning of "Reasonably Usable Form." In *AccessData Corp. v. ALSTE Techs. GmbH* (D Utah, Jan. 21, 2010) 2010 U.S. Dist. LEXIS 4566, *19, the court held that the option to produce ESI in a "reasonably usable form" does not mean that a responding party is free to convert ESI from the form in which it is ordinarily maintained to a different form that makes it more difficult or burdensome for the requesting party to use the information efficiently in the litigation. See *Ch. 9, Gathering and Producing Electronically Stored Information*, 9.50[1].

Sanctions for Failure to Preserve Evidence. In *Jain v. Memphis Shelby County Airport Auth.* (WD Tenn Feb. 25, 2010) 2010 U.S. Dist. LEXIS 16842, the court held that a janitorial service working at an airport, having knowledge of airport procedures for reporting accidents, the existence of a recording system to capture radio communications, and the existence of the surveillance video system used at the airport, had a duty to take steps to ensure that the airport preserved and did not recycle videotapes of a slip-and-fall incident, and granted plaintiff's request for a sanction consisting of a permissive jury instruction that they were allowed, but not required, to presume that the missing videotape would have been unfavorable to the defendants See *Ch. 13, Seeking or Opposing Sanctions for Noncompliance*, 13.04[4].

Federal District Court Imposes Adverse Inferences for Negligent Conduct. In *Pension Committee of the University of Montreal et al. v. Banc of America Securities, LLC et al.* (SDNY January 2010) 2010 U.S. Dist. LEXIS 4546, *6, *105-*107, the court granted an instruction that the jury is permitted to draw an adverse inference about documents that were destroyed through plaintiff's "gross negligence" when the plaintiffs "failed to timely institute written litigation holds and engaged in careless and indifferent collection efforts after the duty to preserve arose." For discussion of the rule in California state and federal courts, see *Ch. 13, Seeking or Opposing Sanctions for Noncompliance*, 13.08[4].



11 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

How to Use Lexis.com(R) With This Publication

1-Chintro MB Practice Guide: CA E-Discovery and Evidence Chintro.syn

§ Chintro.syn Synopsis to Chapter Chintro: How to Use Lexis.com(R) With This Publication

HowTo.01 Finding This Publication and Other Sources on lexis.com.

- [1] Contact LexisNexis(R).
- [2] Using Content Online at lexis.com.
- [3] Selecting a Source on lexis.com.

HowTo.02 Authority and Sources Referenced in This Publication.

- [1] Using lexis.com Resources to Update Cases.
- [2] California Case Databases.
- [3] Hypertext Links.
- [4] Finding Related Sources.
- [5] "Search by Topic or Headnote" Links to Related Cases and Analytical Materials.

HowTo.03 Formulating a Search Query on lexis.com.

- [1] Frame Your Search.
- [2] Develop Your Search Strategy.
- [3] Narrow Your Search.
- [4] Find More Authorities Like This.
- [5] Keep Current With Alerts.

HowTo.04 Shepardize(R) to Validate Your Results and As a Research Tool.



12 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

How to Use Lexis.com(R) With This Publication

1-Chintro MB Practice Guide: CA E-Discovery and Evidence HowTo.01

HowTo.01 Finding This Publication and Other Sources on lexis.com.

[1] Contact LexisNexis(R).

New customers can contact a LexisNexis Account Representative at <http://www.lexisnexis.com/trial/contactrepNALM.asp> or by calling (800) 227-4908.

Current subscribers can reach LexisNexis Customer Support 24/7/365 at (800) 227-4908 or can contact their Account Representative.

[2] Using Content Online at lexis.com. Online subscribers have access to the Total Research System at *lexis.com*. When searching at *lexis.com*, tabs lead users to Legal Sources, Public Records, and News and Business Sources. Additional tabs, such as My Sources and California, can be readily created by the user through the Add/Edit Tabs link directly above the first tab on the left. Sources preceded by a dollar sign and/or an "interrupt" message indicate content outside a subscription plan. These sources may be accessed when available under a customer's alternate transactional pricing plan.

A searchable Directory of Online Sources can be viewed without an ID at <http://web.nexis.com/sources/>.

Additionally, a task-based web page is available for this publication at <http://www.lexisnexis.com/clients/CAPracticeGuide/>.

[3] Selecting a Source on lexis.com.

Use **Source Searches** to select the source you wish to search. For example, on the **Legal** tab see the **States Legal--US** list and follow this jurisdictional path:

California > Search Analysis & CLE Materials > Litigation Practice & Procedure > **Matthew Bender(R) Practice Guide: California E-Discovery and Evidence.**

Content can also be accessed from topical paths related to the publication, e.g.,

Legal Tab > Area of Law--By Topic > Litigation Practice & Procedure > Search Analysis, Law

Reviews & Journals (By State) > California > **Matthew Bender(R) Practice Guide: California E-Discovery and Evidence.**

Use the **Find a Source** tab to locate available paths and sources by entering an exact word or phrase from the source name, or if known, by entering the source library and file. Users may consult the Source Description link following each source (click on the "i" symbol), LexisNexis Customer Support, or the Directory of Online Sources to get information regarding sources, search strategy, or coverage. The standard search price for each source is contained at the bottom of the Source Description page for that source.



13 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

How to Use Lexis.com(R) With This Publication

1-Chintro MB Practice Guide: CA E-Discovery and Evidence HowTo.02

HowTo.02 Authority and Sources Referenced in This Publication.

[1] Using *lexis.com* Resources to Update Cases.

The Matthew Bender(R) Practice Guide series is updated twice a year and cites the strongest, most recent cases available as of its last update. New cases are added to *lexis.com* daily, and can be combined with additional cases online to update, validate, and research fact patterns, issues, and points of law.

[2] California Case Databases.

Numerous sources may assist research needs. They include:

CA Federal & State Cases, Combined (CAL;CAMEGA)

CA Cases, Administrative Decision & Attorney General Opinions, Combined (CAL;CACASE)

CA Published Cases, Combined (CAL;CACTSP)

CA State Cases, Combined (CAL;CACTS) (includes unpublished as well as published cases)

CA Supreme Court Cases from 1850 (CAL;CAL)

CA Courts of Appeal Cases from 1905 (CAL;APP)

Published CA Court of Appeal Cases from 1905 (CAL;APP-P)

Unpublished CA Court of Appeal Cases from 1966 (CAL:APP-U)+[Unpublished CA Court of Appeal Cases from 1966 covers selected unpublished, depublished, and partially published opinions from August 1966 through current, and full coverage of Rule 977 unpublished opinions from October 2001. Although local rules generally preclude citation to unpublished opinions except in limited circumstances, this database may be useful to research similar fact patterns, case information, rulings, factual discovery, strategy, and disposition.]+

Although unpublished cases are not citable in California courts, users may wish to search the CA State Cases,

Combined to get ideas about possible legal arguments. That source would also be preferable to CA Published Cases, Combined if a user is searching for any appellate cases in which a party, attorney, or judge has been involved.

In addition, because of the special importance of federal court decisions in the area of electronic discovery, the following federal sources for both published and unpublished judicial decisions may be of particular value to users of this publication:

Federal Court Cases, Combined (GENFED;COURTS)

U.S. Supreme Court Cases, Lawyers' Edition (GENFED;USLED)

US Courts of Appeals Cases, Combined (GENFED;USAPP)

US District Court Cases, Combined (GENFED;DIST)

9th Circuit--US Court of Appeals, District & Bankruptcy Cases, Combined (GENFED;9TH)

9th Circuit--US Court of Appeals Cases & Bankruptcy Appellate Panel (GENFED;9CIR)

9th Circuit--US District Court Cases (GENFED;9DIST)

Federal Evidence Cases (GENFED;FDEVID)

Case law from all 50 states, the Virgin Islands, Guam, Northern Marianas Islands, Washington, D.C., federal courts, state and federal agencies are also available on *lexis.com* through the Legal tab > Cases - U.S.

[3] Hypertext Links.

Click the hypertext link to jump to the corresponding cases, codes, rules, and other publications online.

[4] Finding Related Sources.

This publication highlights additional online sources to assist your research tasks, both legal and factual, related to pretrial civil procedure. Thousands of additional sources are also available on *lexis.com*.

[5] "Search by Topic or Headnote" Links to Related Cases and Analytical Materials.

Search by Topic or Headnote is a finding tool for legal data based on areas of law and related legal topics. It can help target your legal issue, identify appropriate sources, and formulate your search request.

Some of the search paths in **Search by Topic or Headnote** that are especially relevant to this publication include:

Civil Procedure > Discovery > Methods > Electronic Discovery

Civil Procedure > Discovery > Methods > Requests for Production & Inspection

Civil Procedure > Discovery > General Overview

Civil Procedure > General Overview

Evidence > Authentication > Chain of Custody

Evidence > Demonstrative Evidence > Computer-Generated Evidence

[Evidence > Demonstrative Evidence > Foundational Requirements](#)

[Evidence > Privileges > General Overview](#)

[Evidence > Privileges > Attorney-Client Privilege](#)



14 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

How to Use Lexis.com(R) With This Publication

1-Chintro MB Practice Guide: CA E-Discovery and Evidence HowTo.03

HowTo.03 Formulating a Search Query on *lexis.com*.

[1] Frame Your Search.

After you have selected your source, you can use available tables of contents or enter search terms to retrieve relevant documents. This sample search form provides tips about structuring your search, search connectors, segment searching, and date restrictions.

[Click here to view image.](#)

[2] Develop Your Search Strategy.

Identify relevant terms, their variations, synonyms, necessity, proximity, and relationship to your research issue. Your first search should be structured broadly, then results, can be narrowed without additional search transactions through Focus(R) by adding terms to reduce your search results set.

[3] Narrow Your Search.

Additional parameters, such as Restrict by Segment (field) and Restrict by Date are available. Available Segments are displayed in a dropdown box. For example, the NAME segment of a case contains the names of the parties to the action. To research your adversary's litigation history, you can do a NAME segment search in cases and jury verdicts. You can Add the segment restriction, or type this restriction in your search query as: name (Party Name). Targeted results can also be obtained by restricting the search results to documents that have multiple references to a term or phrase by using ATLEAST#. For example, including *atleast5 (metadata)* as a search term will restrict your search results to documents that reference the phrase "metadata" a minimum of five times.

[4] Find More Authorities Like This.

When you find cases or other documents that are on point to your inquiry and you want to find whether there are other similar materials, you can click the More Like This link at the top of the page. More Like This extracts the relevant search terms for the document you are viewing and gives you the option to use these terms to locate additional materials in the same or a different database. For cases, More Like This can be used to extract citations from an on-point case and use similar citation patterns to locate other cases, treatises, or law reviews. Similarly, the More Like Selected Text link

at the top of documents can be used to target specific paragraphs or language you highlight in an on-point document to locate similar materials. In Case law, More Like This Headnote creates a virtual case law digest online based on the language, law, and topic discussed in headnotes.

[5] Keep Current With Alerts.

To keep your search results current, update your search results by saving an **Alert**. From your online search results screen, select **Save as Alert** link at the top of the screen. You will be given options for how often the search should be run (including daily or weekly) and for how to have the results delivered or a notification sent to you by e-mail.



15 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

How to Use Lexis.com(R) With This Publication

1-Chintro MB Practice Guide: CA E-Discovery and Evidence HowTo.04

HowTo.04 Shepardize(R) to Validate Your Results and As a Research Tool.

Shepardize(R) the cases that you intend to cite to be sure that they are still good law. Additionally, Shepard's can be used as a case-finding and research tool to lead you to other cases, statutes, treatises, and authority on a given issue. You can FOCUS within a Shepard's report on particular terms or phrases. Additionally, the Custom Restrictions link at the top of the Shepard's report allows you to narrow results by jurisdiction, date, and/or headnote restriction. Use the Shepard's Signals to help you analyze validity and subsequent treatment of the case. Shepard's Brief Suite is a free software program to automate Shepardizing your brief or cases, and streamlines the cite checking process for briefs, motions, research, and prior to hearings.



16 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

1- MB Practice Guide: CA E-Discovery and Evidence .syn

§ .syn Synopsis to Chapter : Master Checklist for California E-Discovery

CHECKLIST 1 Determining Use and Extent of E-Discovery in Case.

CHECKLIST 2 Preserving Client's Own Electronically Stored Information.

CHECKLIST 3 Notifying Opposing Party That E-Discovery Will Be Sought.

CHECKLIST 4 Meeting and Conferring Regarding E-Discovery.

CHECKLIST 5 Attending Case Management Conference.

CHECKLIST 6 Obtaining Injunction to Preserve Electronic Evidence.

CHECKLIST 7 Opposing Injunction to Preserve Electronic Evidence.

CHECKLIST 8 Preparing and Making Demand.

CHECKLIST 9 Obtaining Electronic Evidence From Nonparty.

CHECKLIST 10 Preparing Written Response to Electronic Discovery Request.

CHECKLIST 11 Gathering and Producing ESI in Response to a Demand for Production.

CHECKLIST 12 Sample Records Custodian Interview.

CHECKLIST 13 Determining Whether Grounds for Objection to Production of ESI Exist.

CHECKLIST 14 Asserting Objections to Production Demands.

CHECKLIST 15 Seeking Protective Order Against Demand for Electronically Stored Information.

CHECKLIST 16 Opposing Motion for Protective Order.

CHECKLIST 17 Avoiding Monetary Sanctions for Seeking or Opposing Protective Order.

CHECKLIST 18 Obtaining Alternative Relief When Motion for Protective Order Is Denied.

CHECKLIST 19 Moving to Compel Response to Demand for Production of Electronic Evidence.

CHECKLIST 20 Opposing Motion to Compel Response to Demand for Production of Electronic Evidence.

CHECKLIST 21 Moving to Compel Further Response to Demand for Production of Electronic Evidence.

CHECKLIST 22 Opposing Motion to Compel Further Response.

CHECKLIST 23 Moving to Compel Compliance With Statement of Compliance.

CHECKLIST 24 Opposing Motion to Compel Compliance With Statement of Compliance.

CHECKLIST 25 Seeking Sanctions for Noncompliance.

CHECKLIST 26 Opposing Imposition of Sanctions.



17 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

I. INITIAL STEPS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 1

CHECKLIST 1 Determining Use and Extent of E-Discovery in Case.

☐ Is electronically stored information ("ESI") a central element of case?

☐ Are there likely to be e-mails relevant to case?

☐ Are documents relevant to case likely to be stored on a computer or other ESI storage media?

☐ Are other electronic records (such as cell phone call logs) likely to affect issues in case?

☐ How much information relevant to the litigation is likely to exist?

Discussion:

See 4.03-4.10, 6.06

☐ If obtaining ESI is a central element of case, identify ESI that is likely to be sought in discovery, including following details:

☐ Commonly encountered computer-based and other types of ESI and issues they present.

Discussion:

See 1.23-1.43, 9.25

☐ Medium or form in which information likely to be sought is maintained, e.g.:

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 1

- ☐ Computer networks.
- ☐ Servers.
- ☐ Desktop computers.
- ☐ Laptop computers.
- ☐ Cell phones.
- ☐ Blackberries.
- ☐ Personal data assistants (PDAs).
- ☐ Flash drives.
- ☐ Memory sticks and cards.
- ☐ Printers.
- ☐ Backup tapes and other backup media.
- ☐ Other electronic media.

Discussion:

See 6.06, 7.03-7.06

- ☐ Custodian of ESI, either party to litigation or third party.

Discussion:

See 9.12, 9.13, 9.22

Form:

See 9.68

- ☐ Custodian's regular procedures for creating, maintaining, backing up, copying, and deleting ESI.

- ☐ Whether any copies of information are in existence and, if so, where, by whom, and in what form those copies are maintained.

Discussion:

See 4.09[4], 6.03-6.06

- ☐ Determine what information is discoverable.

Authority:

CCP § 2017.010

Discussion:

See 6.05

☐ Review elements of each party's claims and defenses, to determine what facts will be relevant at trial.

☐ Consider information that may be possessed by each party and whether such information will be admissible at trial, or is likely to lead to discovery of admissible evidence.

☐ Consider whether any information possessed by another party is subject to claim of privilege or work-product protection.

- ☐ Determine whether electronically stored information is reasonably accessible, and if not, whether there is good cause for discovery.

Authority:

CCP §§ 2031.010(a), 2031.060

Discussion:

See 6.07[2]

- ☐ Determine whether to demand copy of electronically stored information, or whether to demand testing or sampling of information.

Authority:

CCP §§ 2031.010(a), 2031.060

Discussion:

See 6.07[1], 6.08[1]

- ☐ Determine whether to demand inspection of other party's computer or other devices containing electronically stored information.

Authority:

Dodge, Warren & Peters Ins. Servs., Inc. v. Riley, 105 CA4th 1414, 1417-1418, 130 CR2d 385

Discussion:

See 6.08[2]

- ☐ As soon as possible, learn as much as possible about opposition, including:

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 1

- ☐ Other parties' electronic systems.
- ☐ Other parties' document storage and retention policies.
- ☐ Changes in other parties' software or data storage platforms during time period relevant to litigation.
- ☐ Whether other parties use any specialized computer programs peculiar to their specific type of business.

Discussion:

See 4.09[1]-[4], 5.19[2]

- ☐ Discovery of foreign persons may be available under California code of civil procedure.

Authority:

CCP § 2031.010

Discussion:

See 14.05, 14.06

- ☐ Foreign nationals can request use of Hague Convention for evidence.

Discussion:

See 14.06

- ☐ Jurisdiction must be obtained.

Discussion:

See 14.07

- ☐ If applicable and possible, deal with foreign barriers to pre-trial discovery.

Discussion:

See 14.20-14.24

- ☐ Establish budget for e-discovery.

- ☐ Determine rates charged by all parties who will participate in e-discovery.

- ☐ Establish basic expense categories for budget.

Discussion:

See 4.08[4][b] (cost shifting), 4.17

- ☐ Factor in potential for cost allocation among all parties.

Discussion:

See 5.19[8].



18 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

I. INITIAL STEPS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 2

CHECKLIST 2 Preserving Client's Own Electronically Stored Information.

☐ Understand when duty to preserve evidence arises and the safe harbor provisions of the Electronic Discovery Act:

Discussion:

See 5.05, 5.06

Form:

See 5.26

☐ Preservation duty attaches to any information in custody or control of a party which the party should reasonably know is:

☐ Relevant to action or potential action.

☐ Has been or is likely to be requested during discovery.

Discussion:

See 5.05[1]

☐ Electronic Discovery Act provides a limited "safe harbor" from spoliation claims for routine, good faith operation of an electronic information system.

Discussion:

See 5.05[2]

☐ Parties still have duty to preserve potentially relevant information once litigation is reasonably likely.

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 2

Discussion:

See 5.05[3]

- ☐ Duty to preserve arises when party has notice that the evidence is relevant to litigation or when a party should have known that evidence may be relevant to future litigation.

Discussion:

See 5.05[4]

- ☐ Educate client on legal requirements with respect to e-discovery, importance of compliance, and dangers of noncooperation or failing to take the e-discovery process seriously

**Timing:**

Begin immediately upon receipt of an electronic discovery request or upon reasonable anticipation of litigation.

Discussion:

See 8.05

- ☐ Initiate litigation hold process to preserve client's ESI from routine destruction, in consultation with a project team made up of in-house counsel, client's IT personnel, and, if appropriate, ESI consultant.



Determine whether expert assistance will be necessary or advisable for any of following tasks:

- ☐ Preservation of information.
- ☐ Means of retrieving information so that it can be produced in litigation.
- ☐ Processes by which a computer network operates and is backed up.
- ☐ Steps necessary to make backup tapes readable.
- ☐ Developing search terms reasonably likely to discover relevant evidence.
- ☐ Evaluating and understanding limitations on accessibility that are asserted by other parties.
- ☐ Developing sampling methodologies that can inform a decision about what discovery will be permitted.
- ☐ Ascertaining appropriate costs for e-discovery.

Discussion:

See 4.12-4.14, 5.06, 9.09-9.11, 9.21-26

- ☐ If applicable, determine whether to hire vendor in foreign country for ESI collection.

Discussion:

See 14.28

- ☐ Disseminate document preservation memorandum and subsequent reminders to preserve evidence. Confer periodically with document custodians to confirm compliance.

Discussion:

See 5.07

Form:

See 5.26



19 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

I. INITIAL STEPS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 3

CHECKLIST 3 Notifying Opposing Party That E-Discovery Will Be Sought.

☐ Determine whether there are grounds for an injunction to protect against opposing party's destruction of electronic evidence.

☐ Determine whether information identified as relevant or likely lead to relevant information is at risk of loss or destruction.

Discussion:

See 5.07[2], 7.06-7.08

Forms:

See 7.22, 7.23

☐ Prepare preservation demand.

☐ Preservation demand may be combined with traditional demand letter if given before commencement of litigation.

Discussion:

See 5.11, 5.12

Form:

See 5.28

☐ Include following in preservation demand:

☐ Fact that litigation has been commenced or is imminent.

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 3

☐ General statement of type of evidence claimed to be relevant to claims and defenses.

☐ Demand that all ESI relevant to that stored information be preserved.

☐ Demand that any routine destruction policies that might be applicable to that evidence be immediately suspended.

Discussion:

See 5.12

☐ Send preservation demand to opposing party.

Discussion:

See 5.13



20 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

I. INITIAL STEPS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 4

CHECKLIST 4 Meeting and Conferring Regarding E-Discovery.

- ☐ Negotiate with other parties to set time, date, manner and location for all parties to meet-and-confer regarding e-discovery.

Authority:

Cal Rules Ct, Rule 3.724(8)

Discussion:

See 5.16, 5.16A



Timing:

Must occur at least 30 days before date set for initial case management conference.

- ☐ May be in person or by telephone.
- ☐ May be separate or combined with meet-and-confer to discuss non-ESI issues.

- ☐ Prepare to meet and confer regarding ESI.

Authority:

Cal Rules Ct, Rule 3.724(8)

Discussion:

See 5.19[1]

Form:

See 5.30

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 4

☐ Discuss following issues at conference:

☐ Opposing party's ESI, creation, storage, collection and document retention.

Discussion:

See 5.19[2], 9.17

☐ Form or forms in which information will be produced.

Discussion:

See 5.19[3], 9.17

☐ Time within which information will be produced.

Discussion:

See 5.19[4], 9.17

☐ Scope of discovery of electronically stored information.

Discussion:

See 5.19[5], 9.17

☐ Method for asserting or preserving claims of privilege or attorney work product.

Discussion:

See 5.19[6], 9.18

☐ Method for asserting or preserving confidentiality, privacy, trade secrets, or proprietary status of information.

Discussion:

See 5.19[7], 9.18

☐ How cost of production of electronically stored information is to be allocated among parties.

Discussion:

See 4.18[2], 5.19[8]

☐ Any other issues, including development of a proposed plan for discovery of electronically stored information.

Discussion:

See 5.19[9]

☐ Adopt and document proposed discovery plan.

Authority:

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 4

See *Cal Rules Ct, Rule 3.724*

Discussion:

See 5.19[9]

- ☐ If opposing counsel is not forthcoming, consider propounding interrogatories or noticing a deposition.

Discussion:

See 5.19[10]

Form:

See 5.29

- ☐ Identify areas of agreement and disagreement.

- ☐ Identify areas parties can agree on.

Discussion:

See 5.20[1]

- ☐ Determine if court intervention will be necessary for unresolved issues.

Discussion:

See 5.20[2]

- ☐ Prepare and execute any formal agreements negotiated at conference.

Discussion:

See 5.21



21 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

I. INITIAL STEPS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 5

CHECKLIST 5 Attending Case Management Conference.

- ☐ Comply with meet-and-confer requirements for discussion of issues to be included in the initial case management order.

Authority:

Cal Rules Ct, Rule 3.724

Discussion:

See 5.14-5.21

- ☐ Prepare for initial case management conference by integrating any plan for discovery of electronically stored information with general discovery plan to be presented to court at initial case management conference.

Discussion:

See 5.21, 5.23

- ☐ Attend initial case management conference if required.

Authority:

Cal Rules Ct, Rule 3.722(c), (d)

Discussion:

See 5.23[3]

- ☐ Ask court to include, in initial case management order, any agreements between parties concerning discovery of electronically stored information.

Authority:

Cal Rules Ct, Rule 3.728(13)

Discussion:

See 5.25



22 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

I. INITIAL STEPS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 6

CHECKLIST 6 Obtaining Injunction to Preserve Electronic Evidence.

- ☐ Determine whether to seek injunction by ex parte application.

Authority:

CCP § 527(c); Cal Rules Ct, Rule 3.1202(c)

Discussion:

See 7.10[1], 7.11

☐ Consider whether opposing party is likely to attempt to delete or destroy damaging electronic evidence, and whether party requesting ex parte injunction can make adequate showing to that effect.

☐ Consider whether use of regular noticed motion would result in irreparable harm; for example, by allowing opposing party time to destroy electronic evidence that is essential to movant's case.

- ☐ If proceeding ex parte, prepare necessary documents.

☐ Prepare ex parte application for temporary restraining order.

Authority:

CCP §§ 527(c), 527(d); Cal Rules Ct, Rules 3.1201(1), 3.1202(a), 3.1204(b)(3)

Form:

See 7.16

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 6

- ☐ Prepare affidavits or declarations to establish that great or irreparable injury will result to applicant before matter can be heard on notice.

Authority:

CCP § 527(c)(1); Cal Rules Ct, Rules 3.1201(2), 3.1202(a)

Form:

See 7.17

- ☐ Prepare declaration of applicant's counsel, certifying one of following:

Authority:

CCP § 527(c)(2); Cal Rules Ct, Rules 3.1201(3), 3.1204(b)

Form:

See 7.17

☐ Within reasonable time before application is made, applicant or applicant's counsel informed opposing party or opposing party's counsel at what time and where application would be made.

☐ Applicant or applicant's counsel in good faith attempted but was unable to inform opposing party or opposing party's counsel the application would be made.

☐ For reasons specified in statement, applicant should not be required to provide opposing party or opposing party's counsel advance notice of application.

- ☐ Prepare memorandum in support of application.

Authority:

Cal Rules Ct, Rule 3.1201(4)

- ☐ Prepare proposed order to show cause and temporary restraining order.

Authority:

Cal Rules Ct, Rules 3.1150(c), 3.1201(5)

Forms:

See 7.19

**Timing:**

If proceeding ex parte, unless counsel has reason not to provide opposing party advance notice of application, serve copies of application and accompanying documents at reasonable time, usually no later than 10 a.m. on court day before ex parte appearance.

Authority:

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 6

CCP § 527(c)(2)(A), (C); Cal Rules Ct, Rule 3.1203(a)

- ☐ If proceeding ex parte, file application and accompanying documents, and appear personally in court to present application.

Authority:

Cal Rules Ct, Rules 3.1205, 3.1207

- ☐ If proceeding by noticed motion, prepare necessary documents.

- ☐ Prepare notice of motion and motion for preliminary injunction, including specification of one or both of following grounds for motion:

Authority:

CCP § 526(a); Cal Rules Ct, Rules 3.1110, 3.1112(a)

Discussion:

See 7.12[1][a]

Form:

See 7.20

- ☐ Loss or destruction of electronic evidence described in motion would cause great or irreparable harm to movant, by depriving movant of relevant evidence.

Authority:

CCP § 526(a)(2)

- ☐ It appears that opposing party, by causing or allowing destruction of electronic evidence, is or would be acting in violation of movant's rights, effectively rendering any judgment ineffectual.

Authority:

CCP § 526(a)(3); Dodge, Warren & Peters Ins. Servs., Inc. v. Riley (2003) 105 CA4th 1414, 1418-1419, 130 CR2d 385

- ☐ Prepare memorandum in support of motion.

Authority:

Cal Rules Ct, Rule 3.1112(a)(3)

- ☐ Prepare affidavits or declarations, along with any appropriate exhibits, that are necessary to provide factual support for motion.

Authority:

Cal Rules Ct, Rule 3.1112(b)

- ☐ If proceeding by noticed motion, follow standard motion procedure.

Authority:

Cal Rules Ct, Rule 3.1300 et seq.



Cross Reference:

Matthew Bender(R) Practice Guide: Pretrial Civil Procedure in California, Ch. 26, Law and Motion Practice



23 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

I. INITIAL STEPS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 7

CHECKLIST 7 Opposing Injunction to Preserve Electronic Evidence.

☐ On receipt of notice of motion for preliminary injunction to preserve electronic evidence, or any other notice that discovery of electronic evidence is likely to be sought:

☐ Advise client not to take any steps that could result in loss or destruction of evidence specified in notice.

Authority:

UMG Recordings, Inc. v. Hummer Winblad Venture Partners (In re Napster, Inc. Copyright Litig.) (ND Cal 2006) 462 F Supp 2d 1060, 1069) ; *Zubulake v. UBS Warburg LLC* (SDNY 2003) 220 FRD 212, 216 ; *Cedars-Sinai Med. Ctr. v. Superior Court* (1998) 18 C4th 1, 12, 74 CR2d 248, 954 P2d 511 ; *Dodge, Warren & Peters Ins. Servs., Inc. v. Riley* (2003) 105 CA4th 1414, 1418-1420, 130 CR2d 385

Discussion:

See 7.05

☐ Contact movant's counsel and offer to meet and confer for purpose of resolving issues relating to preservation and discovery of electronically stored information.

Authority:

Cal Rules Ct, Rule 3.724(8)

Discussion:

See 7.14

☐ If issues raised in motion cannot be resolved by conference between counsel, prepare papers opposing motion, including:

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 7

- ☐ Memorandum opposing motion.

Authority:

Cal Rules Ct, Rule 3.1113

Discussion:

See 7.15[1][a]

- ☐ Opposing declarations negating movant's factual allegations of grounds for injunctive relief.

Authority:

CCP § 526(a)(2)-(5)

Discussion:

See 7.15[1][b]

- ☐ File and serve opposing papers.

- ☐ If opposing ex parte application:

Authority:

Cal Rules Ct, Rule 3.1206

Discussion:

See 7.15[2][a]

- ☐ Serve copy of opposing papers on applicant at first reasonable opportunity.

☐ File originals of opposing papers at first reasonable opportunity, or if filing before hearing is impracticable, submit opposing papers to judge at hearing on ex parte application.

- ☐ If opposing noticed motion:

Authority:

CCP §§ 1005(b), 1010.6(a)(6)

Discussion:

See 7.15[2][b]

**Timing:**

File and serve opposing papers at least nine court days before hearing on motion, unless notice of motion was served electronically, in which case time to file and serve opposing papers is extended by two court days.

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 7

☐ Accomplish service in manner reasonably calculated to ensure delivery not later than close of next business day after day on which papers are filed.

☐ Attend hearing on motion.



24 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

II. E-DISCOVERY DEMANDS AND RESPONSES TO DEMANDS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 8

CHECKLIST 8 Preparing and Making Demand.

☐ Determine which form of electronically stored information would be most useful in preparing for trial.

☐ Develop knowledge of common forms of production of ESI, including:

☐ Native file format.

☐ Stored on computers of other locations and may include metadata, or hidden information about a particular document, including its date of creation, author, revisions, and file history.

☐ May be less expensive and is searchable so key terms can be found easily.

Discussion:

See 1.16-1.22, 1.36-1.43, 6.06

☐ Images in PDF and TIFF with a load file.

☐ Replicate a document's image, but they may not include the accompanying metadata.

☐ PDF files may include a searchable text layer that may either be created with the file or added later using optical character recognition. TIFF files are not searchable, but they may be produced with an associated database load file for litigation support software.

Discussion:

See 1.16-1.22, 1.36-1.43, 6.06

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 8

☐ Paper.

☐ Database queries/reports.

☐ Collection of mutually related data/information stored in computer record fields, and can track key business information.

☐ Understand distinction between whether raw data is needed or whether reports created from raw data are needed.

Discussion:

See 1.16-1.22, 1.36-1.43, 6.06

☐ Determine whether electronically stored information is reasonably accessible, and if not, whether there is good cause for discovery.

Authority:

CCP §§ 2031.010(a), 2031.060

Discussion:

See 6.07[2]

☐ Determine whether to demand copy of electronically stored information, or whether to demand testing or sampling of information.

Authority:

CCP §§ 2031.010(a), 2031.060

Discussion:

See 6.07[1], 6.08[1]

☐ Determine whether to demand inspection of other party's computer or other devices containing electronically stored information.

☐ Draft set of demands.

Authority:

CCP § 2031.030(a)(2), 2031.030(b), 2031.030(c)

Discussion:

See 6.11

Forms:

See 6.20, 6.21

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 8

☐ Include following in each demand:

☐ Designation of electronically stored information to be inspected, copied, tested, or sampled, either by specifically describing each individual item or by reasonably particularizing each category of item.

Authority:

CCP § 2031.030(c)(1)

☐  Timing: Specification of reasonable place and time, not less than 30 days after service of demand, for production of demanded information.

Authority:

CCP § 2031.030(c)(2), (3)

☐ Specification of any inspection, copying, testing, sampling, or related activity that is being demanded, manner in which it will be performed, and whether it will permanently alter or destroy item involved.

☐ Form of production, such as native format, TIFF, or PDF, and whether production of metadata is being sought.

Authority:

CCP § 2031.030(a)(2)

Discussion:

See 6.11[h]

☐ Serve set of demands.

Authority:

CCP §§ 2031.020, 2031.040, 2031.290

Discussion:

See 6.12

☐ Review responding party's responses to demands, as well as information produced by responding party.

Authority:

CCP §§ 2031.060, 2031.260, 2031.280

Discussion:

See 6.13

☐ If responding party failed to respond timely, move to compel response.

Authority:

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 8

CCP § 2031.300

- ☐ If necessary, oppose responding party's motion for protective order.

Authority:

CCP § 2031.060

- ☐ If responding party's response is inadequate, consider whether to move for further response.

Authority:

CCP § 2031.310

- ☐ If responding party's production of information is inadequate, consider whether to move for order compelling compliance.

Authority:

CCP § 2031.320

- ☐ If responding party inadvertently produces some information that is subject to claim of privilege or of protection as attorney work product, promptly return that information.

Authority:

CCP § 2031.285



25 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

II. E-DISCOVERY DEMANDS AND RESPONSES TO DEMANDS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 9

CHECKLIST 9 Obtaining Electronic Evidence From Nonparty.

- ☐ Ascertain that electronically stored information sought cannot be obtained from party.

Authority:

Calcor Space Facility, Inc. v. Superior Court (1997) 53 CA4th 216, 225, 61 CR2d 567

Discussion:

See 6.16

- ☐ Prepare subpoena commanding nonparty to produce electronically stored information.

Authority:

CCP § 1985.8

Discussion:

See 6.17

Form:

See 6.22

- ☐ Designate electronically stored information to be inspected, copied, tested, or sampled, either by specifically describing each item or by reasonably particularizing each category of item.

Authority:

CCP §§ 1985.8(a), (j), 2020.410(a), 2031.030(c)(1); *Calcor Space Facility, Inc. v. Superior Court* (1997) 53 CA4th 216, 222, 61 CR2d 567

- ☐ Specify reasonable time and place for production of demanded information, taking care not to

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 9

impose undue burden or expense on subpoenaed person.

Authority:

CCP § 1985.8(j)

Discussion:

See 6.18

- ☐ If desired, specify form in which demanded information is to be produced.

Authority:

CCP § 1985.8(b)

- ☐ Have subpoena served on person to whom it is directed.

Authority:

CCP § 1985.8

Discussion:

See 6.18

- ☐ Review response to subpoena.

- ☐ If subpoenaed person opposes subpoena because of undue burden or expense, demonstrate to court that good cause exists for discovery.

Authority:

CCP § 1985.8(d)-(f)

Discussion:

See 6.19[1]

- ☐ If appropriate, seek sanctions for noncompliance with subpoena.

Authority:

CCP § 1985.8(k)(1), 1992, 2020.240

Discussion:

See 6.19[3]

- ☐ If responding party inadvertently produces some information that is subject to claim of privilege or of protection as attorney work product, promptly return that information.

Authority:

See *CCP §§ 1985.8(i), 2031.285*



26 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

II. E-DISCOVERY DEMANDS AND RESPONSES TO DEMANDS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 10

CHECKLIST 10 Preparing Written Response to Electronic Discovery Request.

- ☐ Analyze discovery request.
 - ☐ Determine if ESI exists and is in client's possession.
 - ☐ Instruct client to make a "diligent search and a reasonable inquiry."
 - ☐ If it is discovered that information is in custody or control of someone else, note that information to be conveyed to requesting party.

Authority:

CCP § 2031.230

Discussion:

See 8.06[1]

- ☐ If applicable, evaluate practical and technical considerations in foreign e-discovery.

Discussion:

See 14.25-14.29

- ☐ Evaluate whether request is overbroad or unduly burdensome.

Authority:

CCP §§ 2031.210, 2017.010, 2017.020, 2031.060(f)

Discussion:

See 8.06[1]

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 10

- ☐ Is all requested ESI relevant to action?
- ☐ Is ESI either admissible in evidence or appears reasonably calculated to lead to discovery of admissible evidence?
- ☐ Does burden, expense, or intrusiveness of requested discovery clearly outweigh likelihood that information sought will lead to discovery of admissible evidence?
- ☐ Can information be obtained from some other source that is more convenient, less burdensome, or less expensive?
- ☐ Is request unreasonably cumulative or duplicative?
- ☐ Does likely burden or expense outweigh likely benefit, taking into account amount in controversy, resources of parties, importance of issues in litigation, and importance of requested discovery in resolving these issues?
- ☐ Assess options for responding to each item or category of request, either:
- ☐ Produce information as requested.
Authority:
CCP §§ 2031.010, 2031.210(1), 2031.060(a)
Discussion:
See 8.07[1]
 - ☐ Object to production in whole or in part.
Authority:
CCP §§ 2031.240
Discussion:
See 8.07[2]
 - ☐ Seek a protective order.
Authority:
CCP § 2031.060
Discussion:
See 8.07[3]; see Ch. 11
- ☐ Assess whether to seek cost shifting or cost sharing.

Authority:

CCP §§ 2031.060, 2031.280(d)

Discussion:

See 8.08

☐ Decide on form in which ESI will be produced:

☐ Form specified in request.

Authority:

CCP § 2031.280

Discussion:

See 8.09[1]

☐ Form in which it is used in ordinary course of business.

Authority:

CCP § 2031.280(c)

Discussion:

See 8.09[2]

☐ Form that is reasonably usable.

Authority:

CCP § 2031.280(c)

Discussion:

See 8.09[3]

☐ Address issues of privileged and confidential information.

☐ Review ESI for privileged and confidential information.

Authority:

CCP § 2031.285(a); Evid Code § 912(a)

Discussion:

See 8.10

☐ Make sure that discovery plan will result in production of responsive ESI in timely manner.

Authority:

CCP §§ 2031.280, 2031.260, 2031.010

Discussion:

See 8.11

- ☐ Review applicable time requirements and plan to make a timely response to discovery request, either:



Timing:

Within 30 days after receiving discovery request; or

Authority:

CCP § 2031.260(a)

Discussion:

See 8.14



- Enter into written agreement with opposing parties to shorten or lengthen response period.

Authority:

CCP § 2031.270

Discussion:

See 8.14

- ☐ Draft written response.



- Immediately below title of case, include identity of responding party, set number, and identity of demanding party.

Authority:

CCP § 2031.210(b)

Discussion:

See 8.16



- Respond to each item or category in demand.

Authority:

CCP § 2031.210

Discussion:

See 8.17



- Each response must be clearly identified, bear same number, and be in same sequence as corresponding item or category in demand.

Authority:

CCP § 2031.210(c)

Discussion:*See 8.18*

☐ Response should state one of following as to each item or category of item:

☐ That party will comply, in whole or part, with the particular demand for inspection and any related activities.

☐ That party lacks the ability to comply with demand for inspection or a particular item or category of item.

☐ An objection to the particular demand.

Authority:*CCP § 2031.210***Discussion:***See 8.17*

☐ Statement of compliance must include statement that:

☐ Production, inspection, and any related activity demanded will be allowed either in whole or in part; and

☐ All documents or things in demanded category that are in possession, custody, or control of that party (if no objection is being made) will be included in production.

Authority:*CCP § 2031.220***Discussion:***See 8.19[1]*

☐ Representation of inability to comply with a particular demand must:

☐ Affirm that diligent search and a reasonable inquiry has been made in order to comply with demand for production.

☐ Specify whether inability to comply is because particular item or category has never existed, has been destroyed, has been lost, misplaced, or stolen, or has never been, or is no longer, in the possession, custody, or control of responding party [*CCP § 2031.230*].

☐ Include the name and address of any natural person or organization known or believed by that party to have possession, custody, or control of that item or category of item [*CCP § 2031.230*].

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 10

Authority:*CCP § 2031.230***Discussion:***See 8.19[2]*

☐ Specify form of production respondent intends to use if:

- ☐ Request did not state a form, or
- ☐ Responding party objects to form specified in request.

Authority:*CCP § 2031.280(c)***Discussion:***See 8.20*

☐ State any applicable objections for each item, category of item, or part of an item or category, for which the responding party has not indicated a willingness to comply or has not represented an inability to comply.

- ☐ Identify with particularity any ESI falling within any category of item to which an objection is being made; and
- ☐ Set forth clearly extent of and specific ground for objection.

☐ If objection is based on a privilege claim, particular privilege invoked must be expressly asserted.

☐ If objection is based on claim that information sought is protected work product, that claim must be expressly stated.

Authority:*CCP § 2031.240(b)***Discussion:***See 8.21*

☐ Have response signed by:

- ☐ Client under oath, unless response contains only objections.
- ☐ Attorney, if response contains any objections.

Authority:*CCP § 2031.250(b), (c)***Discussion:**

See 8.22

☐ Serve response.☐ Serve original on party that made the demand.☐ Serve copies on all other parties to action.**Timing:**

Serve response within 30 days after service of demand unless:

☐ On motion of party making demand, court has shortened time for response, or☐ On motion of party to whom demand has been directed, court has extended time for response.☐ Special rules apply in unlawful detainer actions.**Authority:***CCP § 2031.260***Discussion:**

See 8.23

☐ Do not file response with court.**Authority:***CCP § 2031.290(a)***Discussion:**

See 8.23



27 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

III. PRODUCTION OF ELECTRONICALLY STORED INFORMATION AND OBJECTIONS TO PRODUCTION DEMANDS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 11

CHECKLIST 11 Gathering and Producing ESI in Response to a Demand for Production.

- ☐ Review pleadings in case

Discussion:

See 9.06

- ☐ Negotiate with opposing counsel regarding production of ESI and protection of confidential information.

- ☐ Negotiate issues related to scope of product, form of production, and timing of production with opposing counsel.

Discussion:

See 9.17

- ☐ Protect confidential and proprietary information with stipulated protective orders.

Discussion:

See 9.18

- ☐ Perform and document a diligent search for responsive ESI.

- ☐ Develop a collection plan and document it with an audit trail.

Discussion:

See 9.21

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 11

- ☐ Narrow volume of data to review by carefully targeting and limiting media assets to be harvested.

Discussion:

See 9.28

- ☐ Analyze collected ESI to narrow scope of data to be reviewed for production.

- ☐ Develop an analysis plan.

Discussion:

See 9.31

- ☐ Apply de-duplication techniques to reduce volume of data.

Discussion:

See 9.32

- ☐ Develop systematic and defensible search term strategy to reduce review set to a manageable volume of documents, and, if possible, agree with opposing counsel on that strategy.

Discussion:

See 9.33

- ☐ Develop appropriate queries for gathering ESI from databases.

Discussion:

See 9.35

- ☐ Review for responsiveness and privilege.

- ☐ Choose review methodology and software platform.

Discussion:

See 9.38

- ☐ Evaluate whether to perform case assessment concurrently with review.

Discussion:

See 9.39

- ☐ Develop an effective review procedure.

Discussion:

See 9.40

- ☐ Educate review team about the case and privilege issues.

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 11

Discussion:

See 9.41

- ☐ Identify and segregate privileged information.

Discussion:

See 9.42-9.43

- ☐ Review the remaining documents.

Discussion:

See 9.44

- ☐ Prepare privilege log.

Discussion:

See 9.45

- ☐ Choose an appropriate format for production of ESI.

Discussion:

See 9.49-9.54

- ☐ Negotiate a realistic time for production of ESI.

Discussion:

See 9.55

- ☐ Document each stage of the production.

Discussion:

See 9.56

Form:

See 9.60



28 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

III. PRODUCTION OF ELECTRONICALLY STORED INFORMATION AND OBJECTIONS TO PRODUCTION DEMANDS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 12

CHECKLIST 12 Sample Records Custodian Interview.

- ☐ Interview witness about his or her role in dispute.
- ☐ Note source of any documents witness shows during interview about his or her role in the dispute--this will give preliminary indication of where custodian's relevant documents are likely to reside.
- ☐ Catalog electronic systems used by witness.
 - ☐ E-mail:
 - ☐ How does witness use the company's e-mail system? Does witness regularly sort e-mails into subfolders, and if so, how are subfolders organized in a manner that would enable counsel to make a reasoned, defensible decision to harvest e-mails from only certain subfolders?
 - ☐ How would witness go about searching for electronic documents relevant to case? Are there particular names or terms that would be useful in a search? Are there particular folders or other locations to search? Are there other witnesses to ask?
 - ☐ Does witness back up e-mails onto local hard drive or onto other media such as CD-ROM?
 - ☐ Does witness send relevant documents or e-mails to or from a personal e-mail account, perhaps when working from home?
 - ☐ Does witness know of any relevant information stored on an Internet site (such as

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 12

Internet e-mail services such as Gmail or Yahoo! mail, blogs, document storage or backup sites, Twitter)?

☐ Word processing, spreadsheet and other office documents: What document management system, if any, is used?

☐ Does witness always use organization's document management system?

☐ If not, where does witness store documents?

☐ Working out of office and other media:

☐ Does witness use a laptop?

☐ Does witness use a smart phone or personal digital assistant for work?

☐ Does witness carry or store work on flash disks or thumb drives?

☐ Does witness back up any work information onto portable backup drives, CD-ROM, or older technologies such as Zip drives or floppy drives?

☐ Does witness work from home?

☐ If so, on a company laptop or home computer?

☐ Can any media used by witness be ruled out as not reasonably likely to contain any responsive data?

☐ Has witness used instant messaging, texting, or electronic voice mail systems? Are records of that archived anywhere? Does witness continue to use these systems for data relevant to case?

☐ Did witness receive document preservation instructions? What did witness do in response?

☐ Has any data from relevant time periods been lost for any reason, such as a computer disk crash or migration between computer systems or software? If so, what were circumstances? Can data be retrieved from another source?

**Timing:**

See 9.13[1]

Use and Content of Form:

See 9.13



29 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

III. PRODUCTION OF ELECTRONICALLY STORED INFORMATION AND OBJECTIONS TO PRODUCTION DEMANDS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 13

CHECKLIST 13 Determining Whether Grounds for Objection to Production of ESI Exist.

☐ Review demand for discovery of electronically stored information promptly after receiving it, to determine whether timing or format of demand is objectionable.

☐ If demand is plaintiff's initial demand, consider whether demand was served before expiration of 10 days (five days in unlawful detainer action) after service of summons on, or appearance by, responding party, unless court has granted plaintiff leave to serve demand earlier.

Authority:

CCP § 2031.020(b)-(d)

Discussion:

See 10.05[1]

☐ Consider whether demand was served in time to allow for production of demanded information by discovery cutoff.

Authority:

CCP §§ 2024.020, 2031.030(c)(2)

Discussion:

See 10.05[2]

☐ Consider whether demand fails to designate information sought either by specifically describing each individual item or by reasonably particularizing each category of item.

Authority:

CCP § 2031.030(c)(1)

Discussion:

See 10.05[3]

- ☐ Determine whether any specific demand is objectionable on relevance grounds.

Authority:

CCP §§ 2017.010, 2031.010(a)

Discussion:

See 10.06

- ☐ Determine whether any particular demand is objectionable on grounds of undue burden.

- ☐ Consider whether demand seeks production of information in unreasonable format.

Authority:

CCP § 2031.280(c), (d)

Discussion:

See 10.07[1]

- ☐ Consider whether demand seeks production of information from source that is not reasonably accessible.

Authority:

CCP § 2031.210(d)

Discussion:

See 10.07[2]

- ☐ Consider whether any of following condition exists:

Authority:

CCP §§ 2019.030(a), 2031.060(f)

Discussion:

See 10.07[3]

☐ It is possible to obtain demanded information from some other source that is more convenient, less burdensome, or less expensive.

☐ Discovery sought is unreasonably cumulative or duplicative.

☐ Demanding party has had ample opportunity for discovery in action to obtain

information sought.

☐ Likely burden or expense outweighs likely benefit, considering amount in controversy, resources of parties, importance of issues, and importance of demanded information in resolving issues.

☐ Determine whether any information demanded is subject to claim of privilege or confidentiality.

☐ Consider following privileges and protections:

☐ Attorney-client privilege.

Authority:

Evid Code §§ 954, 955

Discussion:

See 10.08[3]

☐ Attorney work product protection.

Authority:

CCP § 2018.030

Discussion:

See 10.08[4]

☐ Privilege for trade secrets.

Authority:

Evid Code § 1060; see CC § 3426.1(d)

Discussion:

See 10.08[5]

☐ Privilege for official information.

Authority:

Evid Code §§ 1040, 1041

Discussion:

See 10.08[6]

☐ Other constitutional and statutory privileges.

Discussion:

See 10.08[7]

- ☐ Verify that any applicable privilege or protection has not been waived or forfeited.

Authority:

CCP § 2031.300(a); Evid Code § 912; Venture Law Group v. Superior Court (2004) 118 CA4th 96, 105, 12 CR3d 656 ; McKesson HBOC, Inc. v. Superior Court (2004) 115 CA4th 1229, 1239, 9 CR3d 812

Discussion:

See 10.08[2]



30 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

III. PRODUCTION OF ELECTRONICALLY STORED INFORMATION AND OBJECTIONS TO PRODUCTION DEMANDS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 14

CHECKLIST 14 Asserting Objections to Production Demands.

☐ If any particular demand for production of electronically stored information is objectionable, determine manner of asserting objection, either:

☐ In formal response to demand.

Authority:

CCP § 2031.240(b)

Discussion:

See 10.11

☐ By motion for protective order.

Authority:

CCP § 2031.060

Discussion:

See 10.12

☐ If asserting objection in formal response to demand:

☐ Ensure that objection includes all of following:

Authority:

CCP § 2031.240(b)

Discussion:

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 14

See 10.11[1]

Form:

See 8.24

☐ Identification of item or category of information to which objection is made.

☐ Statement of reason or grounds for objection, expressly identifying particular privilege or work-product protection, if applicable.

☐ If objection is based on claim that electronically stored information is from source that is not reasonably accessible, both of following:

Authority:

CCP § 2031.210(d)

☐ Statement that responding party will not search source in absence of agreement with demanding party or court order.

☐ Identification of types or categories of sources of electronically stored information that are not reasonably accessible.

☐ Follow standard procedures for responding to production demand.

Standard Procedure Checklist:

See 8.12

☐ If asserting objection by motion for protective order:

☐ Meet and confer with opposing counsel to resolve objections informally before filing motion for protective order.

Authority:

CCP §§ 2016.040, 2031.060(a)

Discussion:

See 10.12[1]

☐ Follow standard procedures for making motion for protective order.

Standard Procedure Checklist:

See 11.03

- ☐ If timely response to production demand was not filed, seek relief from forfeiture of objections.

Authority:

CCP § 2031.300(a)

Discussion:

See 10.13

Forms:

See 10.15-10.17

- ☐ Prepare and serve response that complies with all applicable statutory requirements other than timeliness.

Standard Procedure Checklist:

See 8.12.

- ☐ Ascertain facts demonstrating that failure to serve timely response was result of mistake, inadvertence, or excusable neglect.
- ☐ Move for relief from forfeiture of objections, following standard procedure for noticed motion.

**Cross Reference:**

Standard format for noticed motion, see *Matthew Bender Practice Guide: California Pre-Trial Civil Procedure*, Ch. 26, 26.39-26.45.

- ☐ Notify every party that received information of claim of privilege and basis for claim.

☐ Confirm party that received privileged information immediately sequesters specified information and either:

- ☐ Returns the information and any copies, or
- ☐ Presents information to the court conditionally under seal for determination of privilege or work product claim.

Authority:

CCP §§ 2031.285(b), 2031.285(d)(1)

**Timing:**

Party receiving privileged information has 30 days to make motion for determination of privilege or work product claim

Discussion:

See 10.14

- ☐ If party receiving privileged information moves for determination of privilege claim, oppose motion.



31 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

IV. PROTECTIVE ORDERS, MOTIONS TO COMPEL, AND SANCTIONS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 15

CHECKLIST 15 Seeking Protective Order Against Demand for Electronically Stored Information.

- ☐ Review demand for discovery of electronically stored information promptly after receiving it, to determine whether protective order may be appropriate.

Authority:

CCP § 2031.060(a)

Discussion:

See 11.04, 11.05

- ☐ Consider whether compliance with demand would cause unwarranted annoyance, embarrassment, oppression, or undue burden or expense.

Authority:

CCP § 2031.060(b)

Discussion:

See 11.05

- ☐ Consider whether demanded electronically stored information is from source that is not reasonably accessible.

Authority:

CCP § 2031.060(c)

Discussion:

See 11.06

- ☐ Consider whether to assert objections in response to demand as alternative to motion for protective order.

Authority:

CCP § 2031.210(d)

Discussion:

See 11.05

- ☐ Meet and confer with opposing counsel to resolve dispute informally before filing motion for protective order.

Authority:

CCP §§ 2016.040, 2031.060(a)

Discussion:

See 11.04

- ☐ If meet-and-confer does not resolve dispute, prepare necessary documents for motion for protective order.

- ☐ Prepare notice of motion and motion for protective order and request for monetary sanctions.

- ☐ If desired, include request for alternative relief should court deny protective order
[see *CCP § 2031.060(d)-(f)*].

Authority:

CCP § 2031.060(a), (b); Cal Rules Ct, Rule 3.1112(a)(1), (2)

Discussion:

See 11.06, 11.07; 11.17-11.19

Form:

See 11.20

- ☐ Prepare memorandum in support of motion.

Authority:

Cal Rules Ct, Rules 3.1112(a)(3), 3.1113

- ☐ Prepare affidavits or declarations, including expert declarations, along with any appropriate exhibits, that are necessary to provide factual support for motion.

Authority:

Cal Rules Ct, Rule 3.1112(b)

Form:

See 11.21

- ☐ Prepare meet-and-confer declaration.

Authority:

CCP §§ 2016.040, 2031.060(a)

Discussion:

See 11.04

- ☐ Prepare proposed order.

Authority:

Cal Rules Ct, Rule 3.1112(b)

Form:

See 11.22

- ☐ Follow standard procedure for noticed motion.

Authority:

Cal Rules Ct, Rule 3.1300 et seq.



Timing:

Motion should be made "promptly" [CCP § 2031.060(b)]



Cross Reference:

Standard format for noticed motion, see *Matthew Bender Practice Guide: California Pre-Trial Civil Procedure*, Ch. 26, 26.39-26.45



32 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

IV. PROTECTIVE ORDERS, MOTIONS TO COMPEL, AND SANCTIONS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 16

CHECKLIST 16 Opposing Motion for Protective Order.

☐ Prepare papers opposing motion for protective order.

☐ Prepare memorandum opposing motion, including following as appropriate:

Authority:

Cal Rules Ct, Rules 3.1112(a)(3), 3.1113

☐ Argument that demanded electronically stored information is reasonably accessible.

Authority:

CCP § 2031.060(c)

Discussion:

See 11.10

☐ Argument that, even if demanded electronically stored information is not reasonably accessible, good cause for discovery exists.

Authority:

CCP § 2031.060(d)

Discussion:

See 11.11

☐ Suggestion of conditions, such as sharing of discovery costs, that court might impose to lessen burden or expense

of discovery.

Authority:

CCP § 2031.060(e)

Discussion:

See 11.12

☐ Request for monetary sanction.

Authority:

CCP § 2031.060(h)

Discussion:

See 11.15

☐ Prepare affidavits or declarations, including expert declarations, along with any appropriate exhibits, that are necessary to provide factual support for opposition.

Authority:

Cal Rules Ct, Rule 3.1112(b)

☐ Follow standard procedure for opposing noticed motion.

Authority:

Cal Rules Ct, Rule 3.1300 et seq.

Discussion:

See Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure, Ch. 26, 26.39-26.45.



33 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

IV. PROTECTIVE ORDERS, MOTIONS TO COMPEL, AND SANCTIONS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 17

CHECKLIST 17 Avoiding Monetary Sanctions for Seeking or Opposing Protective Order.

- ☐ Before motion is made for protective order, engage in good-faith effort to resolve dispute informally, by meeting and conferring with opposing counsel.

Authority:

CCP §§ 2016.040, 2031.060(a)

Discussion:

See 11.14, 11.15[1]

- ☐ Be prepared to propose or accept reasonable compromise of client's position in order to facilitate reasonably cost-effective discovery.
- ☐ Carefully document informal efforts to resolve dispute at meet-and-confer, and describe those efforts in declaration accompanying moving or opposing papers if motion is filed.
- ☐ If court rules against client on motion for protective order, demonstrate any of following:
- ☐ That client acted with substantial justification.

Authority:

CCP § 2031.060(h)

Discussion:

See 11.15[1]

- ☐ That other circumstances make imposition of sanctions on client unjust.

Authority:

CCP § 2031.060(h)

Discussion:

See 11.15[2]

- ☐ If client's motion for protective order was denied, that sanctions are not allowed due to "safe harbor" in that demanded information was lost, damaged, altered, or overwritten as result of routine, good-faith operation of electronic information system.

Authority:

CCP § 2031.060(i)(1)

Discussion:

See 11.15[3]



34 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

IV. PROTECTIVE ORDERS, MOTIONS TO COMPEL, AND SANCTIONS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 18

CHECKLIST 18 Obtaining Alternative Relief When Motion for Protective Order Is Denied.

☐ If court denies motion for protective order based on finding of good cause for discovery:

Authority:

CCP § 2031.060(e), (g)

Discussion:

See 11.12, 11.18

☐ Remind court of evidence, including expert declarations, showing that demanded information is not reasonably accessible because of undue burden and expense.

☐ Make request, either in moving papers or at hearing on motion, that court exercise its discretion to set terms and conditions for production of demanded information, including shifting all or part of cost of discovery to demanding party.

☐ Whether or not court found that demanded information is reasonably accessible, request (either as alternative in moving papers, or orally at hearing) that court limit frequency or extent of discovery of electronically stored information, based on evidence showing any of following:

Authority:

CCP § 2031.060(f)

Discussion:

See 11.19[1]

☐ It is possible to obtain demanded information from some other source that is more

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 18

convenient, less burdensome, or less expensive.

Discussion:

See 11.19[2]

- ☐ Discovery sought is unreasonably cumulative or duplicative.

Discussion:

See 11.19[3]

- ☐ Demanding party has had ample opportunity by discovery in action to obtain information sought.

Discussion:

See 11.19[4]

- ☐ Likely burden or expense of proposed discovery outweighs likely benefit, taking into account amount in controversy, resources of parties, importance of issues in litigation, and importance of demanded discovery in resolving those issues.

Discussion:

See 11.19[5]



35 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

IV. PROTECTIVE ORDERS, MOTIONS TO COMPEL, AND SANCTIONS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 19

CHECKLIST 19 Moving to Compel Response to Demand for Production of Electronic Evidence.

☐ Verify that party to whom demand for production of electronically stored information is directed has failed to serve timely response.

Authority:

CCP §§ 2031.260(a), 2031.300(b)

Discussion:

See 12.05

☐ Review office file and court docket to determine whether court has entered order setting deadline for response to demand for production; if so, verify that response was not served on or before deadline.

Authority:

CCP § 2031.260(a), (b)

☐ In unlawful detainer case, if court has not set deadline for response, verify that no response was served within five days after service of demand for production.

Authority:

CCP § 2031.260(b)

☐ In any other case, if court has not set deadline for response, verify that no response was served within 30 days after service of demand for production.

Authority:

CCP § 2031.260(a)

- ☐ Consider meeting and conferring with opposing counsel to attempt to resolve issues informally, even though "meet-and-confer" declaration is not required for motion to compel when no response has been served.

Authority:

CCP § 2031.300(b)

Discussion:

See 12.04

- ☐ Prepare necessary documents for motion to compel response.
- ☐ Prepare notice of motion and motion to compel response to demand for production, including request for declaration that objections to demand have been forfeited or waived, and request for monetary sanctions.

Authority:

CCP § 2031.300(b), (c); Cal Rules Ct, Rules 3.1110, 3.1112(a)

Discussion:

See 12.06, 12.07[1]

Form:

See 12.32

- ☐ Prepare memorandum in support of motion.

Authority:

Cal Rules Ct, Rules 3.1112(a)(3), 3.1113

- ☐ Prepare affidavits or declarations, along with any appropriate exhibits, that are necessary to provide factual support for motion.

Authority:

Cal Rules Ct, Rule 3.1112(b)

Form:

See 12.33

- ☐ Prepare proposed order.

Authority:

Cal Rules Ct, Rule 3.1112(b)

Form:

See 12.35

- ☐ Follow standard procedure for noticed motion.

Authority:

Cal Rules Ct, Rule 3.1300 et seq.



Cross Reference:

See Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure, Ch. 26, Law and Motion Procedure, 26.39

☐ If motion is denied, demonstrate that moving party acted with substantial justification or that other circumstances make imposition of sanctions on moving party unjust.

Authority:

CCP § 2031.300(c)

Discussion:

See 12.07[2]



36 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

IV. PROTECTIVE ORDERS, MOTIONS TO COMPEL, AND SANCTIONS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 20

CHECKLIST 20 Opposing Motion to Compel Response to Demand for Production of Electronic Evidence.

☐ Obtain documentation of any agreement between parties establishing time for response beyond times specified by statute.

Authority:

CCP § 2031.270

Discussion:

See 12.10

☐ If grounds exist for objection to demand, take steps to establish grounds for court order granting relief from forfeiture of objections.

Authority:

CCP § 2031.300(a)

Discussion:

See 12.11

☐ If late response to demand has been served, verify that response complies with all applicable statutory requirements other than timeliness.

☐ If no response to demand has been served, prepare response that complies with all applicable statutory requirements other than timeliness, and serve response before hearing on motion to compel response.

☐ Ascertain facts demonstrating that failure to serve timely response was result of

mistake, inadvertence, or excusable neglect.

☐ Prepare papers opposing motion.

☐ Prepare memorandum opposing motion, including as appropriate:

Authority:

Cal Rules Ct, Rules 3.1112(a)(3), 3.1113

☐ Request for relief from forfeiture or waiver of objections to demand.

Authority:

CCP § 2031.300(a)

Discussion:

See 12.11

☐ Request for monetary sanction.

Authority:

CCP § 2031.300(c)

Discussion:

See 12.12[2]

☐ Prepare affidavits or declarations, along with any appropriate exhibits, that are necessary to provide factual support for opposition.

Authority:

Cal Rules Ct, Rules 3.1112(b)

Form:

See 12.34

☐ Follow standard procedure for opposing noticed motion.

Authority:

Cal Rules Ct, Rule 3.1300 et seq.



Cross Reference:

See Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure, Ch. 26, Law and Motion Procedure, 26.46

☐ If motion is granted, demonstrate either of following:

Authority:

CCP § 2031.300(c)

Discussion:

See 12.12[1]

- ☐ Opposing party acted with substantial justification.
- ☐ Other circumstances make imposition of sanctions on opposing party unjust.



37 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

IV. PROTECTIVE ORDERS, MOTIONS TO COMPEL, AND SANCTIONS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 21

CHECKLIST 21 Moving to Compel Further Response to Demand for Production of Electronic Evidence.

☐ Determine whether grounds exist for order compelling further response to demand for production of electronically stored information.

☐ Determine whether response to demand is incomplete.

Authority:

CCP § 2031.310(a)(1)

Discussion:

See 12.15[1]

☐ Determine whether representation of inability to comply with demand is inadequate, incomplete, or evasive.

Authority:

CCP § 2031.310(a)(2)

Discussion:

See 12.15[2]

☐ Determine whether any objection asserted in response is without merit or too general.

Authority:

CCP § 2031.310(a)(3)

Discussion:

See 12.15[3]

☐ Determine whether there is good cause for discovery of information sought by demand.

Authority:

CCP §§ 2031.060(c)-(e), 2031.310(b)(1)

Discussion:

See 12.15[4]

- ☐ Determine whether response indicates that information will not be produced in usable form.

Authority:

CCP § 2031.280(c)-(e)

Discussion:

See 12.15[5]

- ☐ Determine whether signature of appropriate individual has been omitted from response.

Authority:

CCP § 2031.250

Discussion:

See 12.15[6]

- ☐ Meet and confer with opposing counsel to attempt to resolve issues informally.

Authority:

CCP §§ 2031.310(b)(2), 2016.040

Discussion:

See 12.16[2]

- ☐ Prepare necessary documents for motion to compel further response.

- ☐ Prepare notice of motion and motion to compel response to demand for production, including request for monetary sanctions.

Authority:

CCP § 2031.310(a), (h); Cal Rules Ct, Rules 3.1110, 3.1112(a)

Discussion:

See 12.17[1]

Form:

See 12.36

- ☐ Prepare memorandum in support of motion.

Authority:

Cal Rules Ct, Rules 3.1112(a)(3), 3.1113

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 21

- ☐ Prepare affidavits or declarations, along with any appropriate exhibits, setting forth specific facts showing good cause justifying discovery sought by demand.

Authority:

CCP § 2031.310(b)(1); Cal Rules Ct, Rule 3.1112(b)

Discussion:

See 12.16[1]

- ☐ Prepare "meet-and-confer" declaration.

Authority:

CCP §§ 2031.310(b)(2), 2016.040

Discussion:

See 12.16[2]

- ☐ Prepare "separate statement" providing all information necessary to understand each demand and all responses to it that are at issue.

Authority:

Cal Rules Ct, Rule 3.1345(a), (c)

Discussion:

See 12.16[3]

- ☐ Prepare proposed order.

Authority:

Cal Rules Ct, Rule 3.1112(b)

Form:

See 12.38

- ☐ Follow standard procedure for noticed motion, ensuring that notice of motion is given within 45 days after service of response to demand, or on or before any later date established by parties' written agreement.

Authority:

CCP § 2031.310(c); Cal Rules Ct, Rule 3.1300 et seq.

Discussion:

See 12.16[4]; see also Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure, Ch. 26, Law and Motion Procedure, 26.39 (checklist for standard motion procedure)

- ☐ If motion is denied, demonstrate that moving party acted with substantial justification or that other circumstances make imposition of sanctions on moving party unjust.

Authority:

CCP § 2031.310(h)

Discussion:

See 12.17[2]



38 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

IV. PROTECTIVE ORDERS, MOTIONS TO COMPEL, AND SANCTIONS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 22

CHECKLIST 22 Opposing Motion to Compel Further Response.

☐ In meeting and conferring with propounding party before motion is filed:

Authority:

CCP §§ 2031.310(b)(2), 2016.040

Discussion:

See 12.16[2]

☐ Determine if informal resolution can be reached on some or all issues.

☐ Make sure that responding party's position on any issue that remains unresolved has substantial justification, so as to avoid sanctions should court ultimately grant motion.

Authority:

CCP § 2031.310(h)

Discussion:

See 12.22[1]

☐ Review motion and copy of response to production demand, to determine whether to contest asserted grounds for motion, on basis of any of following:

☐ Each statement of compliance contained in response to demand is complete.

Authority:

CCP §§ 2031.210(a)(1), 2031.220, 2031.310(a)(1)

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 22

Discussion:

See 12.20[1]

- ☐ Any representation of inability to comply with demand is accurate and includes sufficient explanation and other required information.

Authority:

CCP §§ 2031.210(a)(2), 2031.230, 2031.310(a)(2)

Discussion:

See 12.20[2]

- ☐ Determine whether circumstances support affirmative defense to motion, such as any of following:

- ☐ Propounding party forfeited right to compel further response by failing to give notice of motion within 45 days after service of response, or later date established by parties' written agreement.

Authority:

CCP § 2031.310(c)

Discussion:

See 12.21[1]

- ☐ Information demanded is from source that is not reasonably accessible because of undue burden or expense.

Authority:

CCP § 2031.310(d)-(f)

Discussion:

See 12.21[2]

- ☐ Particular demand that is subject of motion seeks objectionable discovery.

Authority:

CCP §§ 2031.210(a)(3), 2031.240

Discussion:

See 12.21[3]

- ☐ Circumstances such as following justify court order limiting discovery:

Authority:

CCP §§ 2031.060(b), 2031.310(g)

Discussion:

See 12.21[4]

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 22

- ☐ It is possible to obtain demanded information from some other source that is more convenient, less burdensome, or less expensive.
- ☐ Discovery sought is unreasonably cumulative or duplicative.
- ☐ Propounding party has had ample opportunity by discovery in action to obtain information sought.
- ☐ Likely burden or expense of proposed discovery outweighs likely benefit, taking into account amount in controversy, resources of parties, importance of issues in case, and importance of requested discovery in resolving those issues.
- ☐ Limitation on discovery is necessary to protect responding party from unwarranted annoyance, embarrassment, or oppression, or from undue burden and expense.
- ☐ Prepare papers opposing motion.
- ☐ Prepare memorandum opposing motion, including request for monetary sanction.

Authority:

CCP § 2031.310(h); Cal Rules Ct, Rules 3.1112(a)(3), 3.1113.

Discussion:

See 12.22[2]

- ☐ Prepare affidavits or declarations, along with any appropriate exhibits, that are necessary to provide factual support for opposition.

Authority:

Cal Rules Ct, Rule 3.1112(b)

- ☐ Follow standard procedure for opposing noticed motion.

Authority:

Cal Rules Ct, Rule 3.1300 et seq.

**Cross Reference:**

See Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure, Ch. 26, Law and Motion Procedure, 26.39

- ☐ If motion is granted, demonstrate either of following:

Discussion:

See 12.22[1]

☐ That opposing party acted with substantial justification or that other circumstances make imposition of sanctions on opposing party unjust.

Authority:

CCP § 2031.310(h)

☐ "Safe harbor" from sanctions applies because electronically stored information that was demanded has been lost, damaged, altered, or overwritten as result of routine, good-faith operation of electronic information system, and there are no exceptional circumstances justifying sanctions.

Authority:

CCP § 2031.310(j)(1)



39 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

IV. PROTECTIVE ORDERS, MOTIONS TO COMPEL, AND SANCTIONS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 23

CHECKLIST 23 Moving to Compel Compliance With Statement of Compliance.

- ☐ Verify that responding party has failed to produce electronically stored information in accordance with statement of compliance contained in response to demand, as supplemented by statutory requirements and any agreement between parties.

Authority:

CCP §§ 2031.210(a)(1), 2031.220, 2031.280, 2031.320(a)

Discussion:

See 12.25

- ☐ Consider meeting and conferring with opposing counsel to attempt to resolve issues informally, even though "meet-and-confer" declaration is not required for motion to compel compliance with statement of compliance.

Authority:

CCP § 2031.320(a)

Discussion:

See 12.24

- ☐ Prepare necessary documents for motion to compel further response.

- ☐ Prepare notice of motion and motion to compel compliance with statement of compliance, including request for monetary sanctions.

Authority:

CCP § 2031.320(a); Cal Rules Ct, Rules 3.1110, 3.1112(a)

Discussion:

See 12.27[1]

Form:

See 12.39

- ☐ Prepare memorandum in support of motion.

Authority:*Cal Rules Ct, Rules 3.1112(a)(3), 3.1113*

- ☐ Prepare affidavits or declarations, along with any appropriate exhibits, that are necessary to provide factual support for motion.

Authority:*Cal Rules Ct, Rule 3.1112(b)*

- ☐ Prepare "separate statement" providing all information necessary to understand each demand and all responses to it that are at issue.

Authority:*Cal Rules Ct, Rule 3.1345(a), (c)***Discussion:**

See 12.26

- ☐ Prepare proposed order.

Authority:*Cal Rules Ct, Rule 3.1112(b)***Form:**

See 12.41

- ☐ Follow standard procedure for noticed motion.

Authority:*Cal Rules Ct, Rule 3.1300 et seq.***Cross Reference:**

Standard motion procedure, see *Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure*, Ch. 26, *Law and Motion Procedure*, 26.39

- ☐ If motion is denied, demonstrate that moving party acted with substantial justification or that other circumstances make imposition of sanctions on moving party unjust.

Authority:*CCP § 2031.320(b)*

Discussion:

See 12.27[2]



40 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

IV. PROTECTIVE ORDERS, MOTIONS TO COMPEL, AND SANCTIONS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 24

CHECKLIST 24 Opposing Motion to Compel Compliance With Statement of Compliance.

- ☐ Review specific allegations in motion, copy of response to production demand, and documentation of actual production of information, to determine whether motion may be opposed on basis of factual disputes pertaining to matters such as time, format, and cost of production.

Authority:

CCP §§ 2031.270, 2031.280

Discussion:

See 12.30

- ☐ Prepare papers opposing motion.

- ☐ Prepare memorandum opposing motion, including request for monetary sanction.

Authority:

CCP § 2031.320(b); Cal Rules Ct, Rules 3.1112(a)(3), 3.1113

Discussion:

See 12.31[2]

- ☐ Prepare affidavits or declarations, along with any appropriate exhibits, that are necessary to provide factual support for opposition.

Authority:

Cal Rules Ct, Rules 3.1112(b)

- ☐ Follow standard procedure for opposing noticed motion.

Authority:

Cal Rules Ct, Rule 3.1300 et seq.

Discussion:

See Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure, Ch. 26, Law and Motion Procedure, 26.46

☐ If motion is granted, demonstrate either of following:

Discussion:

See 12.31[1]

☐ That opposing party acted with substantial justification or that other circumstances make imposition of sanctions on opposing party unjust.

Authority:

CCP § 2031.320(b)

☐ "Safe harbor" from sanctions applies because electronically stored information that was demanded has been lost, damaged, altered, or overwritten as result of routine, good-faith operation of electronic information system, and there are no exceptional circumstances justifying sanctions.

Authority:

CCP § 2031.310(d)(1)



41 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

IV. PROTECTIVE ORDERS, MOTIONS TO COMPEL, AND SANCTIONS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 25

CHECKLIST 25 Seeking Sanctions for Noncompliance.

☐ Determine whether grounds for sanctions exist.

☐ Has a party deleted or destroyed electronically stored evidence after party reasonably anticipated litigation?

Authority:

CCP § 2023.030; *Keithley v. Home Store.com, Inc.* (ND Cal 2008) 2008 US Dist LEXIS 61741 ; *Zubulake v. UBS Warburg LLC* (SDNY 2003) 220 FRD 212, 218

Discussion:

See 13.04

Forms:

See 13.20-13.22

☐ Has a party altered or destroyed electronically stored evidence *in anticipation of* a discovery request?

Authority:

CCP § 2023.030; *Cedars-Sinai Med. Ctr. v. Superior Court* (1998) 18 C4th 1, 12

Discussion:

See 13.05

Forms:

See 13.20-13.22

☐ Has a party altered or destroyed electronically stored evidence *in response to* a discovery request?

Authority:

CCP § 2023.030; *Cedars-Sinai Med. Ctr. v. Superior Court* (1998) 18 C4th 1, 12

Discussion:

See 13.05

Forms:

See 13.20-13.22

- ☐ Has a third party suppressed or destroyed electronically stored evidence?

Authority:

Temple Cmty. Hosp. v. Superior Court (1999) 20 C4th 464, 477, 84 CR2d 852, 976 P2d 223

Discussion:

See 13.06

Forms:

See 13.20, 13.22-13.23

- ☐ Has a party unsuccessfully made or opposed a motion to compel the production of electronically stored evidence?

Authority:

CCP §§ 2031.300(c), 2031.310(d), 2031.320(b)

Discussion:

See 13.09[1], 13.09[3], 13.09[5]

- ☐ Has a party disobeyed a discovery order?

Authority:

CCP §§ 2031.300(c), 2031.310(e), 2031.320(c)

Discussion:

See 13.09[2], 13.09[4], 13.09[6]

- ☐ Has a party misused inadvertently produced privileged information?

Authority:

Rico v. Mitsubishi Motors Corp. (2007) 42 C4th 807, 817 ; *State Comp. Ins. Fund v. WPS, Inc.* (1999) 70 CA4th 644, 656-657

Discussion:

See 13.10

- ☐ Prepare moving papers:

☐ Notice of motion.

☐ Supporting memorandum.

- ☐ Declaration, if seeking monetary sanction.
- ☐ Separate statement, if seeking issue or evidence sanction.
- ☐ Supporting evidence, if seeking default judgment.
- ☐ Proposed order.

**Timing:**

Motion for sanctions can be filed concurrently with motion to compel (or opposition to motion to compel), or at later time.

Authority:

CCP §§ 585(b), 2023.040; Cal Rules Ct, Rule 3.1345; London v. Dri-Honing Corp. (2004) 117 CA4th 999, 1007-1008, 12 CR3d 240

Discussion:

See 13.12

Forms:

See 13.20-13.22

- ☐ If seeking contempt sanction, prepare declaration or affidavit and order to show cause.

Authority:

CCP §§ 1211(a), 1212, 2015.5

Discussion:

See 13.13

Forms:

See 13.23



42 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

CL Master Checklist for California E-Discovery

IV. PROTECTIVE ORDERS, MOTIONS TO COMPEL, AND SANCTIONS

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 26

CHECKLIST 26 Opposing Imposition of Sanctions.

☐ If motion for sanctions was filed, determine whether grounds exist to object to moving papers or motion procedure.

- ☐ Determine whether notice was sufficient.
- ☐ Determine whether procedure provides for opportunity to be heard.
- ☐ Determine whether motion is in proper form.

Authority:

CCP §§ 2023.030, 2023.040

Discussion:

See 13.15

☐ If monetary sanctions are sought, determine grounds for opposition:

- ☐ Determine whether substantial justification exists for conduct.
- ☐ Determine whether circumstances exist that would make imposition of sanction unjust.
- ☐ Review moving party's declaration and determine whether:

☐ Expenses sought are reasonable and related to discovery abuse described or, rather, punitive, which is inappropriate.

1- MB Practice Guide: CA E-Discovery and Evidence CHECKLIST 26

☐ Reasonable expenses are itemized and explained.

☐ Pro se litigant is seeking reasonable expenses that do not include attorney's fees.

☐ In the case of sanctions against attorney, establish, if applicable, that attorney did not advise conduct.

Authority:

CCP § 2023.030(a)

Discussion:

See 13.15[1]

☐ If issue, evidence, or terminating sanction is sought, determine grounds for opposition:

☐ Consider any mistaken impression or honest confusion that resulted in conduct.

☐ Consider explanation for conduct that would render conduct understandable or less egregious

☐ Consider whether, under circumstances, the less drastic imposition of monetary sanctions would be more appropriate. Be prepared to argue that more serious sanctions sought are too extreme and that lesser sanctions would achieve objective of protecting interests of opposing party.

Authority:

CCP § 2023.030; Hartbrodt v. Burke (1996) 42 CA4th 168, 173, 49 CR2d 562

Discussion:

See 13.15[2]

☐ If order to show cause for contempt was filed with respect to an indirect contempt, determine whether proper procedures were followed:

☐ Determine whether alleged contemner was personally served or whether his or her attorney was served if he or she was avoiding service.

☐ Determine whether alleged contemner is being afforded a full hearing.

☐ Determine whether order to show cause was based on sufficient affidavit.

☐ Consider arguing that less serious sanctions are more appropriate.

Authority:

CCP §§ 1015, 1211(a), 2015.5, 2023.030; Kroneberger v. Superior Court (1961) 196

CA2d 206, 210, 16 CR 339

Discussion:

See 13.15[4]



43 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.syn

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

§ 1.syn Synopsis to Chapter 1: Understanding Electronic Evidence

- 1.01 Scope.
- 1.02 Objective and Strategy.
- 1.03 Resources.
- 1.04 CHECKLIST: Understanding the Risk Areas in Electronic Discovery
- 1.05 Options and Strategies.
- 1.06 Preservation of ESI Can Be Challenging.
- 1.07 Attorneys Must Be Able to Understand and Use Terminology Effectively.
- 1.08 Attorneys Must Be Able to Communicate With Opposing Counsel and Court About ESI Issues.
- 1.09 Attorneys Must Understand What ESI to Seek From Opposing Party, and How to Evaluate Whether a Response to an ESI Demand Is Complete and Accurate.
- 1.10 Attorneys Must Understand How to Use ESI at Trial.
- 1.11 Attorneys Must Stay Current on Developments in E-Discovery.
- 1.12 Attorneys Must Be Concerned About Sanctions.
- 1.13 Attorneys May Need to Retain Experts for Assistance in Understanding and Litigating ESI Issues.
- 1.14 Expert Declarations or Testimony May Be Required.
- 1.15 CHECKLIST: Understanding the Nature and Characteristics of Electronically Stored Information.

1.16 Definition of Electronically Stored Information Is Very Broad.

1.17 ESI Can Be User-Created or Machine-Created.

1.17[1] ESI May Be Created by User or by Operation of Software.

1.17[2] User-Created ESI.

1.17[3] Machine-Created ESI.

1.18 ESI Can Be Stored in Many Locations.

1.19 ESI Can Be Stored in a Variety of Forms.

1.20 ESI Can Be Modified.

1.21 ESI Can Be Deleted, but Traces May Remain.

1.21[1] Deleted Data Defined.

1.21[2] "Deleted" Data May Still Exist and Be Recoverable.

1.21[3] Certain Programs Can Destroy Residual Data.

1.22 ESI Involves Issues Not Encountered in Ordinary Discovery.

1.22[1] ESI Raises Unique Concerns.

1.22[2] Preservation of ESI in Original Form Can Be Difficult.

1.22[3] ESI Contains Hidden "Metadata" That Can Be Critical to Litigation.

1.22[3][a] Metadata Is "Data About Data."

1.22[3][b] "Directory Level" or "System" Metadata.

1.22[3][c] "File-Level" or "Application" Metadata.

1.22[3][d] Embedded Data.

1.22[3][e] Inactive Data.

1.22[3][f] Metadata Can Be "Scrubbed."

1.22[3][g] Need for Metadata and Inactive Data Varies and Must Be Evaluated in Every Case.

1.22[4] Identification of Duplicate Documents Presents Special Issues.

1.22[4][a] E-Mail and Other Programs Facilitate Creation of Multiple Copies of ESI.

1.22[4][b] "Hash Values" Can Be Used to Identify True Duplicates.

1.22[4][c] Near Duplicates Have Minute Changes.

1.22[5] Form of Production Is Important in E-Discovery.

1.22[6] Recovery of Backup Media Can Be Difficult.

1.22[7] Discovery of Legacy Data Can Be Difficult and Expensive.

1.23 CHECKLIST: Understanding Commonly Encountered Types of Computer-Based Electronically Stored Information and the Issues They Present.

1.24 Options and Strategies.

1.25 Operating System and Network Data.

1.25[1] Operating System Directs Overall Computer Activity.

1.25[2] Operating System Provides Date/Time Stamps.

1.25[3] Operating System Creates Chronologies and Activity Logs.

1.25[4] Operating System Creates E-File Metadata.

1.26 Electronic Mail Systems.

1.26[1] E-Mail Process Is Automatic.

1.26[2] E-Mail Terminology: "Client" and "Domain Name."

1.26[3] "Sent" E-Mails Are Transmitted to Recipient Via SMTP Server.

1.26[4] E-Mail Protocols Can Affect E-Discovery.

1.26[5] Most Larger Entities Use Enterprise-Based or Server-Based E-Mail.

1.26[6] Many Individuals Use Internet-Based E-Mail Accounts.

1.26[7] Some Individuals Have Multiple E-Mail Addresses.

1.26[8] HTML E-Mails Have More Functionality Than Text E-Mails.

1.26[9] E-Mails Contain Important Metadata.

1.26[10] Some E-Mail Attachments Are Not Searchable.

1.26[11] Relationships Among E-Mail "Families" Should Be Preserved.

1.27 Calendars and Related Functions.

1.28 Word Processing Programs and Other Document Applications.

1.28[1] Documents May Not Be All Text--Embedded and Referenced Items.

1.28[2] Unprinted Document Text Items.

1.28[2][a] Some Elements in Electronic Documents Will Not Print.

1.28[2][b] Author Comments and Annotations Normally Do Not Print.

1.28[2][c] Redlining and Track Changes Will Not Print on Default Settings.

1.28[2][d] Auto-Date and Automatic Updating Functions May Change Documents.

1.28[2][e] Opening or Printing File Changes File's Metadata.

1.29 Computer Databases.

1.29[1] Databases Are Important in Litigation.

1.29[2] Definition and Types of Databases.

1.30 Spreadsheets.

1.31 Presentation Software.

1.32 Websites.

1.32[1] Websites Can Be Important Sources of ESI.

1.32[2] Wikis.

1.32[3] Blogs.

1.32[4] Intranets.

1.32[5] Internet Browser Records.

1.32[6] Social Networking Sites.

1.33 Voice Mail.

1.34 Videos.

1.35 Instant Messages.

1.36 CHECKLIST: Understanding Other Potential Sources of Electronically Stored Information and the Issues They Present

1.37 Options and Strategies.

1.38 Disaster Recovery Backup Media.

1.38[1] Backup Systems Store Data for Recovery in Event of System Failure.

1.38[2] Different Types of Backup Protocols Are Used.

1.38[3] Backup Data Retention Periods Vary.

1.38[4] Backups May Involve Tape Rotation.

1.38[5] Testing and Sampling May Resolve Disputes About E-Discovery of Backups.

1.39 Hard Drives and Removable Media Can Be Source of ESI.

1.40 Cell Phones and Personal Digital Assistants (PDAs).

1.40[1] Evolution of Technology Has Increased Importance As ESI Source.

1.40[2] Preservation and Recovery of Data Can Be Problematic.

1.41 Third Party Customer Account or Financial Records May Contain Relevant ESI.

1.42 Social or Professional Networking Sites May Contain Relevant ESI.

1.43 Security Data May Contain Relevant ESI.

Appendix A: Glossary of Technical Terms Encountered in E-Discovery.

Helen Marsh n*

Diane E. Barry, Esq. n**

Reviewed by Ernst Halperin n***

FOOTNOTES:

(n1)Footnote *. Helen Marsh is the e-discovery and practice support attorney at the San Francisco firm of Kecker & Van Nest LLP. Helen was an early adopter of technologies and work processes designed to manage large-scale electronic discovery projects, with an eye both to quality and to cost control. She is a frequent presenter at seminars regarding electronic discovery.

(n2)Footnote **. Diane E. Barry, Esq. is the Director of Discovery Strategy & Management at International Litigation Services, Inc. Diane's practice focuses on ESI discovery under state and federal rules of civil procedure, and complex litigation discovery planning and management. Diane assists clients in planning and preparing for ESI discovery conferences and court appearances, as well as preparation for specialized discovery such as IT custodian depositions, key player and IT interviews. In addition, Diane has significant expertise in utilizing technology to improve results in privilege and relevance review. Diane earned her A.B. degree from Vassar College and her J.D. degree, *cum laude*, from the Boston University School of Law. She holds a professional certification in Data Warehousing from U.C. Berkeley.

(n3)Footnote ***. Law Office of Ernst Halperin, San Francisco. Previously a partner with the San Francisco firm of Folger Levin & Kahn LLP, Mr. Halperin has litigated complex commercial, bankruptcy, and intellectual property cases since 1995. He has managed the discovery of ESI in cases alleging breach of merger agreements, trade secret misappropriation, fraudulent transfers, construction defects, and patent infringement. He currently practices as a dispute resolution neutral.



44 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

I. STRATEGY

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.01

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.01 Scope.

This chapter discusses the technology aspects of data storage that bear on the discovery of electronically stored information ("ESI") in California litigation. It is designed to provide attorneys with an understanding of the technology underlying e-discovery, and to enable them to understand the interaction between technology and the legal issues that arise in the e-discovery context. It also is intended to assist attorneys in communicating with technical personnel such as IT specialists, forensic specialists, and e-discovery vendors.

This chapter discusses the following general topics in connection with e-discovery:

- Understanding the attorney risk areas associated with e-discovery [*see 1.04-1.14*].
- Understanding how ESI is stored, deleted, and recovered [*see 1.15-1.21*], and some of the general issues of unique or special concern in e-discovery [*see 1.22*].
- Understanding specific issues encountered with particular types of commonly encountered ESI, including e-mail, word processing documents and similar programs, spreadsheets, computer operating systems, computer databases, websites, and other less frequently used sources of ESI [*see 1.23-1.30*].
- Understanding other sources of ESI, such as backups, removable media, cell phones and personal digital assistants (PDAs), and the special issues that they present [*see 1.36-1.43*].

Appendix A of this chapter is a glossary of technical terms that are frequently encountered in e-discovery, and are used elsewhere in this publication.



45 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

I. STRATEGY

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.02

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.02 Objective and Strategy.

Social norms regarding acceptable channels of communication are changing rapidly. In earlier generations, telegrams and letters were replaced by long-distance telephone calls. Now, telephone calls and facsimile transmissions have been replaced by e-mails, and e-mails in turn are being replaced by text messages, chats, "tweets," and communications on social networking sites. The proliferation of computing, storage, and communication devices in business and personal life has led to enormous volumes of electronically stored information relating to almost any event that might be the subject of civil litigation.

Discovery of electronically stored information is now customary in a wide variety of civil cases. This includes commercial litigation, employment law, family law, and other subject areas.

State and federal courts allow discovery and use of ESI in litigation. In federal court, the framework for discovery of ESI was codified in the 2006 amendments to the Federal Rules of Civil Procedure. In California, the Electronic Discovery Act was passed as an urgency measure and signed by the governor on June 29, 2009 [Stats. 2009, Ch. 5], becoming effective immediately.

Clients, courts and the ethical rules require competence in electronic discovery issues. Attorneys need to be able to advise clients on their ESI obligations in civil litigation. This requires that attorneys understand the basic nature of e-discovery and the basic features of ESI, as well as the major issues and pitfalls that can occur in this area.

Most attorneys and computer/IT specialists come from vastly different professional worlds. The terminology and jargon used by computer specialists is as foreign and incomprehensible to many attorneys as the legal language used by a California litigator would be to an IT specialist. Yet these two types of professionals must be able to communicate in order for effective e-discovery to be conducted. This requires that attorneys have at least a basic understanding of how electronic data storage practices affect the evidence that will be needed to win a case or comply with legal discovery requirements. This chapter provides a basic discussion of that information.



Cross References:

Laws governing e-discovery, see Ch. 2, Governing Law in Electronic Discovery.

Ethical issues, see Ch. 3, Ethical Issues for Attorneys in E-Discovery.



46 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

I. STRATEGY

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.03

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.03 Resources.

A large number of sources exist for information on electronic discovery trends, case law, and technological developments. In fact, most novices find that the resources are so extensive that it can be difficult to identify those that are most useful. The references noted below are often recommended by e-discovery practitioners. While these sources currently focus more on litigation in federal court, they will nevertheless be useful to state court practitioners, given the significant similarities in the law.

- Mealey's Litigation Report: Discovery summarizes key decisions and events relating to electronic discovery.
- Many electronic discovery vendors and at least one law firm have useful information available on line [see, e.g., online law library maintained by vendor at www.applieddiscovery.com; online library maintained by K&L Gates at www.ediscoverylaw.com].
- There are a number of blogs that also assist practitioners to stay abreast of developments in the law.
- The Electronic Discovery Reference Model (EDRM) is a peer-developed approach to electronic discovery. The organization's website is a rich source of information on each of the steps involved in electronic discovery from preservation to production. Moreover, the website contains useful information on some of the most common technical challenges encountered in electronic discovery [see www.edrm.net].
- The Sedona Conference Working Group on electronic discovery has published a number of papers that are often cited by the courts. These papers may be found at the Sedona website [see www.thesedonaconference.org].
- The Federal Judicial Center has published a short guide for use by courts and practitioners alike [see Rothstein, Hedges and Wiggins, *Managing Discovery of Electronic Information: A Pocket Guide for Judges* (Federal Judicial Center 2007)].



47 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

II. UNDERSTANDING THE RISK AREAS IN ELECTRONIC DISCOVERY

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.04

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.04 CHECKLIST: Understanding the Risk Areas in Electronic Discovery

- ☐ Understand attorney risk areas associated with e-discovery.

Discussion:

See 14.04

- ☐ Understand importance and difficulty of preserving ESI.

Discussion:

See 14.05

- ☐ Understand how to communicate clearly and effectively regarding ESI matters.

- ☐ Understand basic ESI and computer terminology relevant to ESI.

Discussion:

See 1.07; see Appendix A

- ☐ Understand how to communicate with opposing counsel and court.

Discussion:

See 1.08.

- ☐ Understand what ESI to seek and how to evaluate ESI demands.

Discussion:

See 1.09

- ☐ Understand how to use ESI at trial.

Discussion:

See 1.10

- ☐ Stay current and up-to-date on recent developments in e-discovery law.

Discussion:

See 1.11

- ☐ Understand the potential for sanctions in e-discovery.

Discussion:

See 1.12

- ☐ Understand the need to obtain technical expertise by retaining experts in e-discovery matters.

Discussion:

See 1.13

- ☐ Understand the importance of expert testimony in e-discovery.

Discussion:

See 1.14



48 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

II. UNDERSTANDING THE RISK AREAS IN ELECTRONIC DISCOVERY

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.05

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.05 Options and Strategies.

In order to conduct successful e-discovery and avoid potential malpractice, sanctions, and ethical issues, it is important that attorneys understand the types of risk associated with e-discovery. Four principal areas of risk are typically associated with e-discovery:

- Failure to find or disclose significant relevant evidence.
- Inadvertent production of privileged or confidential information.
- Inadequate monitoring of processes used.
- Cost overruns from inadequate quality control.



Cross Reference:

The Sedona Conference Commentary on Achieving Quality in the E-Discovery Process, May 2009, www.thesedonaconference.org.



49 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

II. UNDERSTANDING THE RISK AREAS IN ELECTRONIC DISCOVERY

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.06

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.06 Preservation of ESI Can Be Challenging.

It has always been important to act promptly to preserve documents relevant to litigation. With ESI, this is even more critical, as electronic data is ephemeral. It is easily and routinely changed or discarded and even a short delay can be problematic.

Example:

In *Housing Rights Ctr. v. Sterling* (CD Cal 2004) 2004 US Dist LEXIS 28877, the court concluded that a litigation hold was not properly communicated in the absence of declaration from in-house attorney to that effect.

Cross References:

Preservation demands and litigation holds, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferring, Case Management*, 5.03-5.13.

Ethical obligations in connection with litigation holds, see *Ch. 3, Ethical Issues for Attorneys in E-Discovery*, 3.05[4].

Sanctions for failure to produce ESI, see *Ch. 13, Seeking or Opposing Sanctions for Noncompliance*, 13.09.

Corporate records retention policies, see *Ch. 16, Establishing Best Practices Regarding Electronically Stored Information*.



50 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

II. UNDERSTANDING THE RISK AREAS IN ELECTRONIC DISCOVERY

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.07

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.07 Attorneys Must Be Able to Understand and Use Terminology Effectively.

Fluency in the language of electronic discovery is required for communications with courts and opposing counsel, but also for communications with clients, vendors and experts. While there is a developing consensus on the meanings of commonly used terms in connection with ESI, many practitioners are not yet familiar with all of these terms.

Example:

To the technical person, the terms "archives" and "backups" refer to different data sets and are not interchangeable. If attorneys use these terms as if they were interchangeable, there is an increased likelihood of miscommunication.



Cross Reference:

Glossary of technical and e-discovery terms, see Appendix A of this chapter; see also The Sedona Conference Glossary: E-Discovery & Digital Information Management (2d ed.) (December 2007) at www.thesedonaconference.org.



51 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

II. UNDERSTANDING THE RISK AREAS IN ELECTRONIC DISCOVERY

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.08

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.08 Attorneys Must Be Able to Communicate With Opposing Counsel and Court About ESI Issues.

Attorneys will be called upon to provide accurate, complete, and timely information regarding a client's electronically stored information. Inability to communicate can cause problems and generate unnecessary expense.

Examples:

- In *Covad Communs Co. v. Revonet, Inc.* (DDC 2008) 254 FRD 147, the requesting party relied on standard instructions that hark back to the days of all-paper discovery by asking that documents be produced with staples, clips, file folders, and labels intact. The parties had significant disagreements about the form of production for e-mail, all of which could have been avoided by including clear and specific instructions on production of electronic records.

- Attorneys can be criticized for exaggerating costs of certain electronic discovery tasks [see *Toussie v. County of Suffolk* (EDNY 2007) 2007 US Dist LEXIS 93988 (costs to restore backup tapes would exceed \$1 million and process would take over two years)].

- *Best Buy Stores, L.P. v. Developers Diversified Realty Corp.* (D Minn 2007) 2007 US Dist LEXIS 7580 (conclusory statements about costs of compliance with discovery request are insufficient to justify change in schedule)].



52 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

II. UNDERSTANDING THE RISK AREAS IN ELECTRONIC DISCOVERY

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.09

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.09 Attorneys Must Understand What ESI to Seek From Opposing Party, and How to Evaluate Whether a Response to an ESI Demand Is Complete and Accurate.

Even if one's own client does not have an extensive or complex set of ESI, the same degree of knowledge and expertise is required to properly demand ESI from an adverse party. In addition, once ESI has been produced, counsel for the demanding party will need to evaluate that ESI to find relevant information and to determine if the production is adequate.

Strategic Points:



- Because of the volume of electronic data, all parties have an interest in identifying ways to reduce the amount of data that requires an item-by-item review to determine relevance and privilege. Because of the ability to search this data electronically, attorneys and vendors have championed a variety of techniques to do an initial cull of data and thereby screen out certain data as irrelevant. Electronic data collection and review software often provides the ability to perform keyword searches. Commonly used criteria for reducing the amount of data to be reviewed also include date restrictions, file types, keywords or search terms, custodians, and duplicates. More recently, software vendors have started to implement the ability to perform "conceptual searches" across data populations. Conceptual search software uses special algorithms to group or cluster together search results based upon similarity of concepts in the data files, so users can quickly identify related files and eliminate groups of non-relevant files. Each of these approaches is dependent on an understanding of the technology in play.

- Disputes regarding the form of production of electronically stored information have dominated the early litigation on e-discovery. Most discussion about the form of production centers around one central issue: should electronically stored data be produced in "native" format? For a native production, Outlook e-mail message would be produced as .pst files, a Microsoft format for archived e-mail messages. Excel files would be produced as Excel files and viewable as such on any computer. And if files will not be produced in native format, what form will they be produced? The key considerations are the ability to provide metadata with non-native production formats, and the ability to provide fully searchable text

with non-native production formats.



Cross References:

Review and production of ESI, see Ch. 9, *Gathering and Producing Electronically Stored Information*.

Discussion of metadata and "native format" production, see 1.22, *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing and Case Management Conference*, 5.19[3], *Ch. 9, Gathering and Producing Electronically Stored Information*, 9.25, 9.53-9.54.



53 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

II. UNDERSTANDING THE RISK AREAS IN ELECTRONIC DISCOVERY

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.10

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.10 Attorneys Must Understand How to Use ESI at Trial.

There are special issues to consider in connection with the authentication of ESI [see, e.g., *Lorraine v. Markel Am. Ins. Co.* (D Md 2007) 241 FRD 534 (providing roadmap to authentication issues that arise with respect to a number of types of ESI); *People v. Hawkins* (2002) 98 CA4th 1428, 1450, 121 CR2d 627 (analysis of evidentiary issues for admission of computer clock times)].



Cross Reference:

See Ch. 15, Admissibility of Electronic Evidence at Trial.



54 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

II. UNDERSTANDING THE RISK AREAS IN ELECTRONIC DISCOVERY

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.11

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.11 Attorneys Must Stay Current on Developments in E-Discovery.

There are hundreds of opinions relating to electronic discovery issues. Many or most of the rulings regarding these issues are unreported. This presents additional challenges for practitioners, particularly in view of the constant changes in technology that have implications for electronic discovery.

Example:

In *Smith v. Cafe Asia* (DDC 2007) 2007 US Dist 73071, plaintiff was ordered to preserve and produce images on a cell phone.



55 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

II. UNDERSTANDING THE RISK AREAS IN ELECTRONIC DISCOVERY

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.12

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.12 Attorneys Must Be Concerned About Sanctions.

Sanctions have been threatened or imposed on attorneys who have been involved in cases in which electronic data has been withheld or lost. As courts and litigants become more involved in the resolution of disputes regarding ESI, there is a greater potential for failures to be viewed as malfeasance rather than misfeasance. Moreover, federal courts have imposed sanctions on attorneys in cases in which electronic discovery problems were identified.

Examples:

- In *Qualcomm Inc. v. Broadcom Corp.* (SD Cal Jan 7, 2008) 2008 US Dist LEXIS 911 , the court imposed sanctions against six outside attorneys who ignored warning signs that document productions were inadequate; moreover, the attorneys were reported to the State Bar of California for investigation.
- In *Preferred Care Partners Holding Corp. v. Humana, Inc.* (SD Fla 2009) 2009 US Dist. LEXIS 30523 , counsel was characterized as "grossly negligent," "careless," and showed "bad judgment" in failing to identify and produce key documents and metadata.
- In *Bray & Gillespie Mgmt. LLC v. Lexington Ins. Co.* (MD Fla Mar. 4, 2009) 2009 U.S. Dist. LEXIS 21250 , the court raised the issue of sanctions against in-house and outside counsel due to "willful blindness" regarding availability of metadata.
- In *L.H. v. Schwarzenegger* (CD Cal 2008) 2008 US Dist. LEXIS 86829 , sanctions were imposed for late production of ESI and producing non-sortable PDFs.
- In *Lombardo v. Broadway Stores* (Cal App 4th Dist. 2002) 2002 Cal App Unpub LEXIS 4700, 1-2 , sanctions were imposed for destroying the electronic form of requested payroll records that were also produced in paper form.



56 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

II. UNDERSTANDING THE RISK AREAS IN ELECTRONIC DISCOVERY

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.13

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.13 Attorneys May Need to Retain Experts for Assistance in Understanding and Litigating ESI Issues.

One of the challenges in the area of electronic discovery is determining when to obtain the support of experts. There are a number of firms that have formed practice groups for electronic discovery issues, yet those groups may consist primarily of individuals who are conversant on the legal issues relating to e-discovery, but not as familiar with the technical issues.

Strategic Points:



- Even when a firm has significant expertise, it may not be desirable to rely on firm employees to handle technical tasks. Thus, while law firm employees may be well versed and well trained in the use of electronic discovery or forensic software, the day-to-day responsibilities of those individuals may not involve the use of all of the types of software available. Moreover, because factual issues regarding the preservation, collection and processing of ESI often become issues in the litigation, counsel may prefer to have client or expert witnesses not affiliated with counsel's law firm as the witnesses with respect to these factual issues.

- When sanction or waiver issues arise in connection with ESI, counsel's use of an expert in handling complex ESI issues may be considered by the court in considering the reasonableness of counsel's actions [see, e.g., *Rhoads Indus. v. Bldg. Materials Corp. of Am. (ED Pa 2008) 254 FRD 216* (counsel's use of an expert and specialized software in searching for privileged documents were factors in finding that production of privileged materials was inadvertent)].

Example:

A case may involve ESI from a cell phone or from web-based e-mail accounts, and the best way to preserve and collect such ESI may be unfamiliar to counsel. In such cases, it is desirable to retain a vendor or expert to implement related aspects of the electronic discovery plan.



Cross References:

Discussion of e-discovery experts, see *Ch. 4, Planning E-Discovery, 4.11-4.14*; *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing and Case Management Conference, 5.06*.



57 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

II. UNDERSTANDING THE RISK AREAS IN ELECTRONIC DISCOVERY

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.14

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.14 Expert Declarations or Testimony May Be Required.

If e-discovery issues are presented to the court because of a controversy in need of resolution, an outside expert may be in a better position to submit declarations or provide testimony.



Strategic Point:

A firm may not want an employee to provide expert opinion and become subject to deposition or other challenge.

Example:

In a criminal matter, the court suggested that expert may be needed to construct an effective list of search terms [*see, e.g., United States v. O'Keefe* (DDC 2008) 537 F Supp2d 14, 24] .



58 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

III. UNDERSTANDING THE NATURE AND CHARACTERISTICS OF ELECTRONICALLY STORED INFORMATION

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.15

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.15 CHECKLIST: Understanding the Nature and Characteristics of Electronically Stored Information.

- ☐ Understand comprehensive nature of definitions of ESI.

Discussion:

See 1.16

- ☐ Understand basic characteristics of electronically stored information.

- ☐ ESI can be either user-created or machine-created.

Discussion:

See 1.17

- ☐ ESI can be stored in many locations.

Discussion:

See 1.18

- ☐ ESI can be stored in different forms.

Discussion:

See 1.19

- ☐ ESI can be modified.

Discussion:

See 1.20

- ☐ ESI, or evidence that the ESI once existed, sometimes can be recovered even though the ESI has been "deleted."

Discussion:

See 1.21

- ☐ Understand issues that are unique or especially significant in e-discovery.

- ☐ Preservation in original form can be difficult.

Discussion:

See 1.22[2]

- ☐ ESI contains hidden "metadata" that may contain information crucial to litigation.

Discussion:

See 1.22[3]

- ☐ Process of identifying and removing duplicate documents can be more difficult, time-consuming, and expensive in e-discovery than ordinary discovery.

Discussion:

See 1.22[4]

- ☐ Form of production is a key issue in e-discovery.

Discussion:

See 1.22[6]

- ☐ Recovery of backup media can present technical difficulties and be expensive.

Discussion:

See 1.22[6]

- ☐ ESI may exist in form of "legacy" data that may be difficult and expensive to recover.

Discussion:

See 1.22[7]



59 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

III. UNDERSTANDING THE NATURE AND CHARACTERISTICS OF ELECTRONICALLY STORED INFORMATION

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.16

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.16 Definition of Electronically Stored Information Is Very Broad.

The legal definitions of ESI are very broad. In California, the Electronic Discovery Act defines "electronically stored information" as "information that is stored in an electronic medium" [CCP § 2016.020(e)]. The word "electronic" is defined as "relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities" [CCP § 2016.020(d)].

Compare--California Definitions Are Consistent With Federal Approach: This broad definition in California statute is consistent with the approach taken in the Federal Rules of Civil Procedure. Although the Federal Rules contain no definition of ESI, Rule 34 provides that a party may request electronically stored information that is "stored in any medium" [Fed R Civ Proc, Rule 34(a)]. Moreover, the Advisory Committee describes ESI as "information that is stored in a medium from which it can be retrieved and examined." The Committee further states that "Rule 34(a)(1) is expansive and includes any type of information that is stored electronically." Moreover, the rule is intended to reach "future developments in computer technology" [Advisory Committee comments to Fed R Civ Proc, Rule 34 Subdivision (a)].



60 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

III. UNDERSTANDING THE NATURE AND CHARACTERISTICS OF ELECTRONICALLY STORED INFORMATION

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.17

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.17 ESI Can Be User-Created or Machine-Created.

1.17[1] ESI May Be Created by User or by Operation of Software. There are two principal kinds of ESI. The first, user-created ESI, is created by a user, and is familiar to most people who use computers. The second kind of ESI, machine-created ESI, is created by the operation of the computer software, and many users are unfamiliar with the types and volumes of machine-created ESI that exist.

1.17[2] User-Created ESI. User-created ESI is sometimes referred to as "active data" because the user actively creates the records. This is the type of ESI that is created by most commonly used software programs, including word processing documents, spreadsheets, and PowerPoint presentations.



Warning:

Some user-created data, often called "embedded data," can be hidden in some views of a document. When printed, embedded data generally is not visible. Care should be taken to choose a method of data production that does not lose this data.

Examples:

- An Excel spreadsheet may contain hidden formulas, rows, columns, or comments.
- A PowerPoint presentation may have notes viewable only by the presenter.
- A Word document may have tracked changes or a comment feature.

1.17[3] Machine-Created ESI. Machine-created data includes both file-level metadata and system-level metadata, and is sometimes referred to as "application data" or "system data." When a user creates a document using word processing software, for example, certain information will be automatically recorded regarding that document. This

information is recorded without any instruction from the user, and, in many instances, the user will not fully understand or appreciate the fact that this data is being created and in some cases retained in association with the document.

This data will generally include information such as the date and time a document is created, revised or printed. It is the actual or perceived need for this type of data that drives the discussion about the discoverability of metadata.

**Cross Reference:**

Discussion of metadata, see 1.22[3].



61 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

III. UNDERSTANDING THE NATURE AND CHARACTERISTICS OF ELECTRONICALLY STORED INFORMATION

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.18

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.18 ESI Can Be Stored in Many Locations.

ESI can be found in numerous locations. Even sophisticated users may not be aware of all of these locations. Storage methods and locations, and the type of ESI stored, will depend upon the hardware and the software being used. Examples of different hardware are a Windows PC, an Apple computer, a cell phone, or a network server. Storage methods and locations include the following:

- Storage in temporary or transient forms (such as computer RAM during typing, storage in Internet caches as e-mail is transmitted).
- Disk drive storage.
- Networks for storage.
- External/physical media (tapes, disks, flash drives).
- Internet servers.
- Local copies of files (offline e-mail cache, local copies of documents downloaded from a website).

File or document management software can also control how and where data is stored, and what other metadata about the file is stored in an associated database record. Examples of commonly used document management systems include Hummingbird, PCDocs, DocsOpen.



62 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

III. UNDERSTANDING THE NATURE AND CHARACTERISTICS OF ELECTRONICALLY STORED INFORMATION

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.19

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.19 ESI Can Be Stored in a Variety of Forms.

ESI generally is stored in a format that facilitates the creation, modification, and retrieval of data and information. The formats include the following:

- **Files that can be read by a particular application** (for example, a file with a *.doc or *.docx extension indicates a MS Word file). Other common application document types include Excel spreadsheet files (typically carrying an *.xls extension).
- **Images of documents.** The two major image formats for images of documents are Tagged Image File Format ("TIFF") and Portable Document Format ("PDF").
- **Images only.** The major format for digital photographs is known as JPEG. This format is commonly used for graphics and photographs. Although an image may contain words, a JPEG image is not word-searchable. Thus, for example, a JPEG image of a proposed product warning label may be critical in a product liability case, but the text of the label will not be part of a text search using search terms or keywords.
- **Files with both images and text** (such as PDF files that include a text layer).
- **Temporary Internet files.** An Internet storage or cache file is a temporary area on a drive where data is stored for future use. This is done without active direction by the user [*see, e.g., Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey (ED Pa 2007) 2007 US Dist LEXIS 52544* (court held that the defendant's automatic but unintentional deletion of cache files did not constitute spoliation); *Inventory Locator Serv., LLC v. Partsbase, Inc. (WD Tenn 2006) 2006 US Dist LEXIS 39521* (web server logs allegedly fabricated to support claim made in litigation)].
- **Random access memory (RAM).** RAM is memory that is used by a computer program temporarily during a computer process, and then written over when it is no longer needed. It may be possible to instruct the computer program to save the contents of RAM to a more permanent storage location where

it may be copied and produced in discovery [*see, e.g.,* Columbia Pictures Indus. v. Bunnell (CD Cal June 19, 2007) 2007 US Dist LEXIS 46364 ; (CD Cal Aug 24, 2007) 2007 US Dist LEXIS 63620 (in copyright infringement action, court held that defendant must turn on logging feature of server in order to preserve records of internet file requests)].

■ **Audio files** (such as .wav). This will include call center and voice mail data. As audio files have become digitized, they have been less expensive to store. As with other types of electronic records, many more audio files are retained or can be readily retained as the ease and low cost of storage has improved. For example, audio files are becoming increasingly prevalent as companies implement integrated voice mail systems that send a digital recording of the voice mail message to the user's e-mail in-box. They are most commonly in a format known as "Waveform Audio Format," also known as "Audio for Windows." The files typically can be identified because they have a *.wav extension. Another common audio format is the now ubiquitous "MP3" format used by music players. In discovery, review of digital audio files can be very expensive and difficult due to the need for individually listening to each file. To address this problem, vendors are developing technologies for performing automated searches of audio files [*see, e.g.,* Swarz, "Listen Up and Discover Audio Recordings," Legal Tech Newsletter, February 25, 2009]. This may foretell an increased interest in the retention, processing, review, and production of this type of electronic record.



63 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

III. UNDERSTANDING THE NATURE AND CHARACTERISTICS OF ELECTRONICALLY STORED INFORMATION

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.20

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.20 ESI Can Be Modified.

Merely turning on a computer or accessing ESI to view it can change some types of ESI. For example, directory-level metadata includes information identifying when a file was last accessed. This is not always important, for example, in cases in which file access times are not important, but if it is important, collection of this ESI must be done with expert assistance in order to prevent inadvertent modification of this metadata [see, e.g., *Gates Rubber Co. v. Bando Chem. Indus.* (D Colo 1996) 167 FRD 90, 112-113 (discussing how forensic data recovery by expert should be done)].

ESI can be modified by automatic computer processes and by operator commands on a computer file, such as by saving a file. Indications of modification may include:

- Last save metadata.
- Track changes.
- Versioning software.
- Existence of other non-modified versions of the file.



64 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

III. UNDERSTANDING THE NATURE AND CHARACTERISTICS OF ELECTRONICALLY STORED INFORMATION

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.21

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.21 ESI Can Be Deleted, but Traces May Remain.

1.21[1] Deleted Data Defined. Deleted data is data that once existed as active data but that has been marked as deleted.



Warning:

Note that the definition of "deleted data" is *not* synonymous with "data that no longer exists." As discussed below, deleted data often *does* continue to exist, and may be accessed.

Data may be deleted in two ways:

- First, files or data may be deleted manually by a user. Manual deletion occurs when a user deletes a file or data set. It may happen intentionally or inadvertently.
- Second, files or data may be deleted by computer processing that is integral to the operating system. System-controlled deletions often result from normal and necessary computer operations.

Other system-generated deletions may be controlled by an IT group for a variety of reasons. For example, deletion protocols can result in the deletion of all e-mail in a user's "sent" folder after 30 days. Attorneys must inquire into these protocols and ensure that they are modified as appropriate to prevent inadvertent destruction of potentially relevant ESI once litigation that may call for this ESI is reasonably anticipated.

Example:

- A court imposed significant sanctions on a defendant for failing to end the auto-delete function that destroyed all e-mails that were older than 60 days [*see United States v. Philip Morris USA, Inc. (DDC 2004) 327 F Supp2d 21*] .

■ A company's policy of periodically overwriting all e-mails due to limited network capacity and relying on individual employees to store e-mails relevant to litigation did not qualify for "good faith" safe harbor to avoid sanctions under Fed R Civ Proc 37 [*Phillip M. Adams & Assocs., L.L.C. v. Dell, Inc.* (D Utah Mar 27, 2009) 2009 US Dist LEXIS 26964] .



Cross References:

Document retention policies, see Ch. 16, Establishing Best Practices Regarding Electronically Stored Information.

Litigation holds, see Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference.

Sanctions for failure to preserve evidence, see Ch. 13, Seeking or Opposing Sanctions for Noncompliance.

Ethical issues, see Ch. 3, Ethical Issues for Attorneys in E-Discovery.

1.21[2] "Deleted" Data May Still Exist and Be Recoverable. Deletion of ESI may not mean that the data is really gone. A file pointer may just be erased, but some or all of the file may still be recoverable. Data from documents or files that have been deleted generally remain on a hard drive until the space is used to store other data. Thus, significant content may be recoverable from the "unallocated" or "slack" space.

When a user deletes a file by using the delete command in her personal computer's operating system software, or by dragging its icon into the "trash" or "recycle" folder on the desktop and then choosing the "empty trash" command, the only immediate consequence is that the file no longer appears in the computer operating system's list of files. The file itself remains stored in the hard-disk sectors where it was originally saved. However, the space that the deleted file occupies is flagged as available for storage of new data. Over time, new data will be stored in those spaces and the original content of the file will be lost. This process can take some time, and fragments of files may be recoverable for some time after deletion. If a forensic copy of the hard disk is made and then searched, these fragments of files may be found and used as evidence in litigation [see, e.g., *Dodge, Warren & Peters Ins. Services, Inc. v. Riley* (2003) 105 CA4th 1414, 1417-1418, 130 CR2d 385 (ordering imaging and search of hard disks for deleted files)].



Strategic Point:

If deleted data is important to the case, it will often be desirable to obtain a forensic image of a hard drive. This will preserve both the active data as well as any data in the slack space.

1.21[3] Certain Programs Can Destroy Residual Data. Certain programs will destroy fragments of deleted data, either as an intended purpose of running the program or as a by-product of another operation.

Some programs are intended to completely overwrite deleted files to make the files unrecoverable. While there may be a legitimate data security reason to run such a program (such as preventing unauthorized access to data on computers that are being sold), the use of such a program during or before litigation may be evidence that the user has intentionally deleted files and may expose the user to sanctions [see, e.g., *Electronic Funds Solutions, LLC v. Murphy* (2005) 134 CA4th 1161, 1183-1184, 36 CR3d 663 (terminating sanction entered, after defendants repeatedly failed to comply with discovery orders and intentionally destroyed electronically stored information requested by plaintiffs by running a program to erase e-mails from computer hard drives); *Communications Center, Inc. v. Matthew Hewitt, et al.* (ED Cal 2005) 2005 US Dist LEXIS 10891 ; *Kucala Enterprises Ltd. v. Auto Wax Co.* (ND Ill 2003) 2003 US Dist LEXIS 8833]

Other computer programs can also write over deleted data. For example, if a user runs certain utilities such as a disk de-fragmentation program, residual data often will be destroyed. During the normal operation of a microcomputer, the operating system saves the fragments of a file (for example, a word file or a program file) to different sectors on the hard drive. These sectors may or may not be adjacent to each other. When the information in a single file is spread over disk sectors that are far apart, the computer spends more time accessing the hard drive to obtain the data. Defragmenting programs operate by rearranging where the file fragments are stored--to the extent possible, storing fragments from the same file on adjacent hard-drive sectors. This process destroys residual data.

**Cross References:**

Ethical issues, see Ch. 3, Ethical Issues for Attorneys in E-Discovery.

Sanctions, see Ch. 13, Seeking or Opposing Sanctions for Noncompliance.



65 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

III. UNDERSTANDING THE NATURE AND CHARACTERISTICS OF ELECTRONICALLY STORED INFORMATION

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.22

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.22 ESI Involves Issues Not Encountered in Ordinary Discovery.

1.22[1] ESI Raises Unique Concerns. Discovery involving ESI raises questions that have no direct analogy in the traditional production of paper documents, and these questions are most likely to lead to discovery disputes.

- Challenges relating to the implementation of effective litigation holds that cover all forms of ESI [see 1.06].
- The presence of metadata [see 1.22[3]].
- The proliferation of duplicates [see 1.22[4]].
- Questions relating to the form of production for various types of ESI [see 1.22[5]].
- What to do about data that may be less accessible or inaccessible, including backup and legacy data [see 1.22[6], 1.22[7]].

1.22[2] Preservation of ESI in Original Form Can Be Difficult. It is often difficult to preserve ESI in an unaltered form even assuming that relevant ESI is identified correctly at an early stage in a dispute. If, for example, litigation relates to a party's ongoing business, it may be difficult to keep up with the retention and collection of ESI. As each new document is created, edited, saved or discarded, one must consider whether each iteration must be retained for litigation purposes.

1.22[3] ESI Contains Hidden "Metadata" That Can Be Critical to Litigation.

1.22[3][a] Metadata Is "Data About Data." "Metadata" is the term for information generated by the operating system and other software programs, and attached to a particular computer file. It is often described as "data about data." Metadata helps the creating program store, track, and access the target data file. Once generated, metadata is embedded in the target file and made part of it. Metadata does not ordinarily print out as part of the printed document.

Compare:

One way to think about metadata is to compare it to the old physical index cards libraries used. When a library acquired a book, a tracking number was applied to the book itself (usually on the spine) and the book was usually stamped somewhere to show it was the property of the library. The librarian would find a place for the book on the library's shelves, and an index card would be generated. The index card had basic information on a particular book so that it could be identified among all of the other books (title, author, publisher, blurb). Then the card would list where the book could be found on the library shelves. Metadata tracks this same kind of basic information on particular electronic files--when it was created, who created it, when it was last modified, where it stored, and other similar information. The particular metadata fields available are different for different kind of files. For example, the metadata for an e-mail will list the date and time it was sent, whether it was read by the recipient, etc. An MS Excel file is not sent, so the operating system does not have "sent" data for this kind of file. However, the OS does probably track the last time the Excel file was modified.

Metadata is an integral part of the ESI file, and the most knowledgeable courts are treating it as such. This means that it should be considered as included in an ESI request whether the discovery demand requests it specifically or not [*see Williams v. Sprint (D KS 2005) 230 FRD 640* ("when 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"); *but see Aguilar v. Immigration and Customs Enforcement Division of the U.S. Dept. of Homeland Security (SDNY 2008) 225 F.R.D. 350* (plaintiff who did not specify form of production or ask for metadata in its first request for production had to pay for defendant's costs of producing Word and PowerPoint files a second time if plaintiff wanted the metadata)].

**Strategic Points:**

- Metadata is of interest in ESI discovery because it can be useful in de-duplicating and culling a data set so that fewer documents require review and analysis, and in case analysis, to understanding more about a particular document and its relevance to the case. Even if the other side doesn't want it, the producing party wants it. It is useful and saves costs.
- Conversely, no one needs all the available metadata. For example, e-mail files can have 50-plus available fields of metadata. Counsel should discuss what fields are available with the forensic collection vendor, make a list of those fields that are relevant and useful, and be prepared to offer those fields to opposing counsel at the meet and confer meeting conducted prior to the case management conference.

Consider:

Metadata normally is entirely computer generated. However, it is possible for users to supplement metadata for certain types of data files. Microsoft Word files stored in Microsoft Windows are an example. If the user right-clicks on a Word document icon and selects "Properties" and then selects "Summary," the metadata generated by the operating system for a Word document is displayed. However, there is space in that screen where the user can supplement the computer-generated information and add a summary or other notes about the document. This is not the norm, but it is possible.

1.22[3][b] "Directory Level" or "System" Metadata. "Directory level" or "system" metadata is metadata about electronic files that is supplied by the computer's operating system (OS). It usually pertains to e-files such as spreadsheets, word processing files, Power Points, etc. These are all files that reside directly on a computer hard

drive--in the area governed by the OS. The basic metadata generated can be seen by right-clicking on a document icon and selecting "properties." System metadata, such as time stamps, will take their information from the settings in the OS. Whatever the OS clock says will be taken for the time stamp. This can differ from the time stamps generated by programs working on the same computer. It is possible to use time settings in programs different from those that are on the computer OS.

Examples--Directory-Level Metadata:

Examples include "create date," "last modification date," and "last access date."



Strategic Point:

Usually, when ESI data is processed for review, the vendor asks the producing party to select an available date or time stamp for THE date time stamp. The system date is often the most reliable. This is an item to discuss with the vendor or ESI consultant.

1.22[3][c] "File-Level" or "Application" Metadata. "File-level" or "application" metadata is the metadata unique to the file type. Just as the operating system creates metadata to permit it to track and account for a computer file, each program that makes data files also creates metadata to assist it in working with the file. The metadata created by the application will differ with the kind of application. For example, e-mail programs create a great deal of metadata because of the travels of an e-mail in and out of its system. Word processing programs will make other kinds of metadata.

Example--File Level Metadata:

The following are some of the types of metadata associated with Microsoft Word documents:

- User's name.
- User's initials.
- User's company or organization name.
- The name of the user's computer.
- The name of the network server or hard disk where the user saved the document.
- Other file properties and summary information.
- The names of previous document authors.
- Document revisions.
- Document versions.
- Template information.
- Hidden text or cells.
- Personalized views.

■ Comments.

Different types of file types will have their own unique file-level metadata associated with them. Documents in Portable Document Format (PDF) will have different file-level metadata from, for example, Excel spreadsheets or the output of computer-aided design programs used in architects' offices. Consultants knowledgeable in electronic discovery should be able to help counsel understand the metadata associated with each file type, so that counsel can make an informed decision about whether file-level metadata is likely to be important in the case.

1.22[3][d] Embedded Data. Document files can consist of more than text data. Document files can include almost any kind of ESI--sound files, accounting data that updates from the corporation's accounting system, animations, movie files, music, and others. Embedded information may or may not print out well. An animation doesn't print out; neither do sound files.

Documents can also include notes and annotations that do not print out. They do not show in the native file unless the user places his or her mouse over the appropriate spot on the "page." In all of these cases, the full impact of the ESI document information may be available only in the original native file.

1.22[3][e] Inactive Data. "Inactive data" is data that has been deleted or modified. Inactive data still resides on the computer's hard drive, but is not accessible to the operating system. The operating system's directory now identifies the sectors on which inactive data reside as available for more data.

Example--Inactive Data:

A common example of "inactive data" is files on a personal computer that the user has deleted using either operating system commands or by dragging into the "trash" or "recycle" folder on the desktop and then "emptying" the trash.

1.22[3][f] Metadata Can Be "Scrubbed." It is not uncommon for corporations to use metadata scrubbing programs as part of their e-mail protocols. This process "wipes" the metadata for all attached documents, removing confidential or privileged information, such as the fact that a document was originally drafted by counsel. When a document is produced without any metadata, a question can arise as to whether the metadata simply was not collected, or was "scrubbed." Counsel can avoid questions along these lines by alerting opposing parties to the fact that certain parties or persons used metadata scrubbers.

1.22[3][g] Need for Metadata and Inactive Data Varies and Must Be Evaluated in Every Case. In the e-discovery context, metadata disputes have been widely publicized. Metadata can be important when there are questions concerning authenticity of a document, or who worked on a particular document is likely to be relevant to a case.

Consider:

In general, metadata is less important when the *contents of the document itself*, and not *the activity of the user*, is the main concern in the litigation. The more important the activity of the user is to issues in the case, the more important metadata and inactive data become. Some techniques for collecting ESI alter metadata, or fail to collect inactive data. Understanding and properly evaluating the potential relevance of metadata and inactive data to the issues in the case will enable counsel to choose the appropriate collection methods.



Strategic Point:

Counsel will save time and money by asking for exactly what is needed, and no more. Counsel should consider the importance of metadata in each case, and for each type of ESI. Counsel should also consider

what types of metadata are *relevant* in each case, and for each type of ESI.

 Cross Reference:

Discussion of utilizing appropriate collection methods to preserve metadata and inactive files if necessary, see *Ch. 9, Gathering and Producing Electronically Stored Information*, 9.26.

1.22[4] Identification of Duplicate Documents Presents Special Issues.

1.22[4][a] E-Mail and Other Programs Facilitate Creation of Multiple Copies of ESI. The existence of multiple copies of the same document presents problems in a paper production. In an electronic production, the problems are compounded.

Example:

An e-mail from one individual to 10 recipients can exist in at least 11 mailboxes. These e-mails will not be considered duplicates because of that fact. Although technically they are not duplicates, the question of whether to produce these "near duplicates" (11 copies of the one e-mail sent to 10 recipients) is frequently encountered by counsel. A decision not to produce some of the near duplicates may lead opposing counsel to conclude that the witnesses have been destroying evidence, either inadvertently or on purpose. On the other hand, reviewing duplicative e-mails wastes time and money, given that attorney review time is often the most expensive cost in producing ESI.

Electronic discovery processing and review software (and services) commonly provide the user with the ability to identify exact duplicates (identical in all respects), and "near duplicates," and to treat them in batches so that only one exemplar in any given set of "near duplicates" need be reviewed.

1.22[4][b] "Hash Values" Can Be Used to Identify True Duplicates. True duplicates can be identified by use of "hash values" or "hashing." A hash value is an alphanumeric string of digits automatically assigned to a file according to its characteristics by use of a mathematical algorithm. MD5 is one of the commonly used hashing algorithms, although there are others. A hash value is often referred to as an "electronic document fingerprint." The most minute change in the contents of a document or its metadata will result in assignment of a different hash value to the altered file. By comparing hash values, it is possible to eliminate identical, true duplicates from a population at issue. Electronic discovery processing and review software (and services) commonly use the MD5 hash to identify true duplicates.

Strategic Point:



In a production of documents in native form, the hash value can be a stand-in for the more traditional Bates number applied on a page-by-page production of documents in paper or near-paper format. However, hash numbers can include 32 digits of information, making them unwieldy as document identifiers. Nevertheless, the technology for using hash values is advancing, and solutions to this problem will no doubt be found, increasing the usefulness of native productions.

 Cross Reference:

Discussion of applying de-duplication techniques to reduce the volume of data, see *Ch. 9, Gathering and Producing Electronically Stored Information*, 9.32.

1.22[4][c] Near Duplicates Have Minute Changes. "Near duplicates" are documents that, to the reader, may appear to be duplicates because they have the same text, but are not true duplicates, since they may have minute changes. They are files that are very similar, but not identical to each other.

Some vendors of electronic discovery processing and review software utilize proprietary algorithms to identify "near

duplicates." These software packages often allow users to set the similarity threshold for segregating "near duplicates."

1.22[5] Form of Production Is Important in E-Discovery. "Form of production" refers to the format used for documents produced in response to a discovery demand. Generally, this is a topic for the meet and confer.

 Cross Reference:

Discussion of meet and confer conference, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference, 5.14-5.21.*

The demand may specify the form or forms of production [*CCP* § 2031.020(a)(2)], but the responding party can object and specify in the response the form in which it intends to produce the ESI [*CCP* § 2031.280(c)]. If a demand for production does not specify a form or form in which the ESI must be produced, the producing party can elect to produce the documents in the form in which they are ordinarily maintained, or "a form that is reasonably useable" [*CCP* § 2031.280(d)].

The most common forms of production (in rough order) are:

- TIFF or PDF with a database load file (sometimes called "near paper").
- Native format.
- Paper.
- Conversion of the ESI to another useable electronic form.

"TIFF or PDF with a database load file" ("near paper") means that the ESI is converted to images of pages in either TIFF or PDF format, often with Bates numbers and confidentiality legends on the image. Each imaged page has corresponding entries in the database load file with data from the original ESI. For example, if the ESI is an e-mail, the image will be a printout of the e-mail, whereas the load file entry will have data associated with that e-mail in searchable and sortable fields (fields such as sender, recipients, subject line, date, identification of attachments, full searchable text of the e-mail, or custodian of the e-mail).

Native format is a copy of the original electronic file. For example, e-mail from an Outlook e-mail program would be produced in a *.pst file. Native format files include the metadata of the original file. Native format files also are easy to modify. This presents difficulties in being able to easily ensure that the data is not altered after being produced. Cooperation of counsel and well-documented procedures are required to allow effective use of native format evidence at depositions and trial.

ESI can also be printed out on paper. However, without agreement of counsel, paper should not be used as a form of production because it will be less searchable and sortable than the original ESI [*see, e.g., Lombardo v. Broadway Stores* (2002) 2002 CA Unpub LEXIS 4700, 1-2 (sanctions imposed for destroying electronic form and producing paper form)].

ESI can also be produced by conversion to other forms of ESI that are produced in lieu of the original ESI. For example, information from a database may be exported to a text file or an Excel spreadsheet.

 Cross Reference:

See *Ch 9, Gathering and Producing Electronically Stored Information, 9.54.*

1.22[6] Recovery of Backup Media Can Be Difficult. Backup tapes are created and retained in order to facilitate

recovery of data lost due to an unforeseen event, such as a natural disaster or a system failure.

The *Zubulake* cases raised the question of the discoverability of data residing only on backup tapes [*Zubulake v. UBS Warburg, LLC*, (SDNY 2003) 217 FRD 309, 2003 US Dist LEXIS 7939 ("Zubulake I") (legal standard for determining the cost allocation for producing e-mails contained on backup tapes); *Zubulake v. UBS Warburg, LLC*, (SDNY 2003) US Dist LEXIS 7940 ("Zubulake II") (addressing reporting obligations); *Zubulake v. UBS Warburg LLC*, (SDNY 2003) 216 FRD 280 ("Zubulake III") (allocation of backup tape restoration costs); *Zubulake v. UBS Warburg, LLC* (SDNY 2003), 220 FRD 212 ("Zubulake IV") (preservation duties)]. This has prompted a great deal of subsequent litigation and commentary of the need to preserve, review, and produce relevant material on backup media.

Traditionally, the most common medium for backup of system data has been backup tape, although with the price of hard-drive storage rapidly dropping, hard drive-based backup media are becoming more common. Backup tapes are created and retained in order to facilitate recovery of data lost due to an unforeseen event, such as a natural disaster or a system failure. This type of "disaster recovery" backup medium generally is not designed to be used for archival purposes, nor is it intended for use in litigation. During normal business operations of an enterprise, disaster recovery tapes generally are reused on a periodic rotating basis.

"Accessible backup media" refers to backup media (usually tapes), which are actively used for information retrieval. An example would be tapes holding car rental records from an automobile rental company's rental records database.

Particular problems involving backup data include the following:

- **Preservation of tapes can present challenges and expense.** Preservation of backup tapes can be costly, as it requires a party to retain indefinitely a large volume of data. Disaster recovery backup tapes are usually recycled to a fixed schedule. Courts recognize that the cost of preserving disaster recovery backup tapes can be prohibitively expensive with the potential to cripple an organization, and treat them differently from backup tapes that are actively used for information retrieval by an enterprise.

- **Limitations on utility.** There are limitations to backup media. The tape can deteriorate, and it may not all survive processing. If large numbers of tapes are available, it may be impossible to find the important data through sampling. If only a small number of tapes are available, it may be that the important data has not been retained, and the backup effort will not yield favorable results.

Cross Reference:

Discussion of dealing with archived data, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferring, and Case Management Conference*, 5.06[7].

1.22[7] Discovery of Legacy Data Can Be Difficult and Expensive. Legacy data describes ESI that was created and/or stored with older computer hardware or software that is no longer used by the organization. It differs from backup data in that legacy data is not retained for disaster recovery purposes. In some instances, such legacy data is not subject to any records retention program, but has simply been kept by the organization without any analysis of the information.

Examples:

An example of legacy data would be old backup tapes in a format that is different from the format currently used by the company's IT department. Another example might be an old server running Lotus Notes when the enterprise has switched to a Microsoft Exchange server and migrated the active e-mail data to new hardware.

Particular problems involving legacy data include:

- **Inadequate description.** In many instances in which legacy data exists, there is inadequate information about its content. For example, one may find a large number of unlabeled "floppy disks," but have no information about the data on the disks.

- **Locating necessary hardware and software can be difficult and expensive.** The hardware or software needed to evaluate legacy data may be difficult to find, and it is generally necessary to engage a consultant. Reconstruction of this data may be costly.



66 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

IV. UNDERSTANDING COMMONLY ENCOUNTERED TYPES OF COMPUTER-BASED ELECTRONICALLY STORED INFORMATION AND THE ISSUES THEY PRESENT

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.23

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.23 CHECKLIST: Understanding Commonly Encountered Types of Computer-Based Electronically Stored Information and the Issues They Present.

- ☐ Understand basic functions of a computer operating system and what kind of ESI it will contain.

Discussion:

See 1.25

- ☐ Understand how e-mail systems work and what e-discovery issues e-mail presents.

Discussion:

See 1.26

- ☐ Understand how computer calendars and related functions can affect e-discovery.

Discussion:

See 1.27

- ☐ Understand how word processing programs and other document applications work, and what special e-discovery issues they present.

Discussion:

See 1.28

- ☐ Understand how spreadsheets and other computer databases work, and what special e-discovery issues they present.

Discussion:

See 1.29

- ☐ Understand how presentation software works and what potential e-discovery issues it presents.

Discussion:

See 1.30

- ☐ Understand how Internet websites work and how data stored on such sites can be important in e-discovery.

Discussion:

See 1.32

- ☐ Understand potential use of voice mail in e-discovery.

Discussion:

See 1.33

- ☐ Understand application of video technology to e-discovery.

Discussion:

See 1.34

- ☐ Understand how instant messaging works and its potential in e-discovery.

Discussion:

See 1.35



67 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

IV. UNDERSTANDING COMMONLY ENCOUNTERED TYPES OF COMPUTER-BASED ELECTRONICALLY
STORED INFORMATION AND THE ISSUES THEY PRESENT

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.24

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.24 Options and Strategies.

Computer-based ESI comes in many forms, and each of these forms presents its own distinct issues. In order to understand and successfully conduct discovery, an attorney must have at least a basic understanding of how each of these computer-based ESI sources functions. First is the operating system, which directs the computer's overall activity [see 1.25]. After that, there are numerous individual applications. Electronic mail programs (e-mail) are probably the most important overall source of ESI, and attorneys need to understand how these systems work and how they should be addressed in e-discovery [see 1.26]. Next are word processing and similar applications that are used to create and preserve letters, memos, contracts, and other important documents [see 1.27]. Also important are databases (spreadsheets) [see 1.30] and presentation software [see 1.31]. Websites can be an important source of ESI [see 1.32], and other formats such as voice mail, videos, and instant messages also are potential sources [see 1.33-1.35].



68 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

IV. UNDERSTANDING COMMONLY ENCOUNTERED TYPES OF COMPUTER-BASED ELECTRONICALLY STORED INFORMATION AND THE ISSUES THEY PRESENT

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.25

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.25 Operating System and Network Data.

1.25[1] Operating System Directs Overall Computer Activity. An operating system is software that directs the overall activity of a computer (e.g. MS-DOS, Windows, Linux, and others). The nickname for an operating system is "OS." The computer defaults to the OS when it "boots up." A user will access or launch all other programs through the operating system. Looked at another way, the operating system is the platform upon which all the other computer programs rest. The OS supports them and lets them operate on the computer without interfering with each other. Programs communicate with the computer through the OS. For example, the OS decides where files will be saved, so that different programs don't try to save data into the same places.

1.25[2] Operating System Provides Date/Time Stamps. The OS also provides certain kinds of information that is used by the programs it supports. One such example is date and time stamps. The date/time of the OS is usually the date/time the program uses when it autofills those items in its files.

1.25[3] Operating System Creates Chronologies and Activity Logs. An OS keep tabs on what is happening on a computer and when, including:

- When did someone log in?
- What programs did they access while they were logged in?

This OS data is useful because it can provide a base timeline of what a computer was doing and when, and this information is difficult for the ordinary user to get, let alone change or falsify. The problems are that the OS keeps this kind of data for only a short period of time. It is created and kept for the OS's own purposes, and it is not needed for long.

1.25[4] Operating System Creates E-File Metadata. The OS also creates information to permit it to track e-documents stored on its hard drive:

- Where are particular files kept on the hard drive?
- When did they log out?

It can also track information on a file:

- When was it created?
- Who created it?
- When was it last modified?

This is the "metadata" that is stored with a document. It is the information the OS created to keep track of the file. It is comparable to a library index card: there is some essential information to help the OS recognize the file and find its parts, so that when someone wants it, it can assemble the file and pull it up on command.



69 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

IV. UNDERSTANDING COMMONLY ENCOUNTERED TYPES OF COMPUTER-BASED ELECTRONICALLY STORED INFORMATION AND THE ISSUES THEY PRESENT

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.26

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.26 Electronic Mail Systems.

1.26[1] E-Mail Process Is Automatic. E-mail can be distributed from an individual machine to locations around the world. This happens seamlessly and instantaneously. As such, most users never are required to understand how this is accomplished. There are a variety of protocols in use that determine what will happen when a user creates an e-mail message and then hits the "send" button.

1.26[2] E-Mail Terminology: "Client" and "Domain Name." An understanding of basic e-mail terms is necessary to discuss how e-mail works:

- An e-mail "client" is the software or service used by the end user to send and receive e-mail.

Examples:

If a litigant uses Outlook e-mail, then Microsoft Outlook is that litigant's e-mail client. Similarly, if a user has an AOL account, then AOL is that user's e-mail client.

- A "domain name" is the portion of an e-mail address that identifies the organization or computer that is used for e-mail communications.

Examples:

Microsoft.com, jonescollege.edu, gmail.com, and smithfamily.com are examples of domain names.

1.26[3] "Sent" E-Mails Are Transmitted to Recipient Via SMTP Server. When the end user creates a new e-mail using his or her e-mail client and hits the "send" button, the message is first transmitted to the SMTP server. (SMTP stands for "Simple Mail Transfer Protocol.") This is a server maintained by the enterprise that is host to a domain. The e-mail is then delivered to the recipient in one of the following ways:

- If the e-mail is addressed to someone at the same domain as the sender, the SMTP server transmits

the message to that person.

- If that person resides at a remote location, then the e-mail is sent via the Internet.
- If an e-mail is sent to a recipient with a different domain name, then the host SMTP server will communicate via the Internet to identify the Internet protocol address of the SMTP server for the recipient's domain.

1.26[4] E-Mail Protocols Can Affect E-Discovery. There are a number of ways (known as "protocols") that an e-mail can be transmitted over the Internet to an addressee's e-mail in-box. There are differences in these protocols that can have implications for records retention and e-discovery purposes.

The principal issue relates to the location of the e-mail messages. In some instances, an e-mail message remains on an Internet server even after a recipient views the message. In others, e-mail messages are downloaded to the recipient's local machine, and do not remain on the Internet server.



Warning:

However, users have the ability to change these processes, and, as a result, it is necessary to investigate all possible storage locations for each mailbox of interest.

The types of e-mail protocols are:

- **Post Office Protocol (POP).** This is the oldest method of distributing e-mail over the Internet. When users connect to their online mail servers, POP downloads all e-mail messages to the local machine. With the default settings, the e-mail is deleted from the mail server and the e-mails reside only on the local hard drive.
- **Internet Mail Access Protocol (IMAP).** This is the protocol for Lotus Notes, as well as other applications. With IMAP, when users check their mailboxes, the body of the e-mail is not downloaded to the local hard drive. Rather, only the message header ("to," "from," subject, date) is downloaded to the local drive. When an e-mail is opened, the body is accessed on the online IMAP server. Thus, the e-mail messages remain on the server even after they have been deleted from the hard drive. Moreover, even if not deleted, only the header information will normally be found on the hard drive, absent changes to the default settings. However, many users will synchronize their local drives with the IMAP server in order to read and answer e-mails while not online. IMAP and other server-based protocols make it easier to access e-mail from multiple locations rather than a single machine.



Strategic Point:

It may not be important in many cases to understand the e-mail protocols, procedures or practices in place at a given time. However, it is sometimes necessary to know where copies of incoming and sent messages are kept under normal circumstances. This will depend in large part on the e-mail protocol in use.

1.26[5] Most Larger Entities Use Enterprise-Based or Server-Based E-Mail. Most midsize or larger entities will use an enterprise e-mail client that is managed via an IT group.

Messaging Application Programming Interface (MAPI) is the proprietary e-mail protocol used by Microsoft's Exchange Server application. It will be relevant to any organization that uses Exchange. With MAPI, e-mails are stored on the

Exchange server. The Exchange server may be located in the same physical location as a user, although that is not required. The local hard drive does not have fully replicated e-mail inboxes or folders.

A user can, of course, copy e-mails or folders to a hard drive, and in fact, in most instances, archived e-mail will be stored only on the hard drive.

1.26[6] Many Individuals Use Internet-Based E-Mail Accounts. Many individuals use web-based or browser-based e-mail for personal use, with programs such as Gmail or Hotmail.

- HTTP is an abbreviation for Hyper Text Transfer Protocol. With this application, all e-mail and related information is stored on the server. Unless a user has saved items to a drive, data will generally not be found on the local machine.
- Increasingly, web-based applications are predominating. Gmail and Hotmail offer all the features of the expensive systems, virtually unlimited online storage, and the ability to access files from any location at any time with no special equipment.

1.26[7] Some Individuals Have Multiple E-Mail Addresses. Some individuals have multiple e-mail addresses, perhaps with different domain names, that are used for particular time periods or specific functions. For example, a person might use one e-mail address for Internet shopping and the like, but have another one for family or personal correspondence. This is done in part to protect a user from spam and other unsolicited messages. In addition, an individual may switch to a new e-mail client but keep the old account active. It is therefore important to identify all possible e-mail addresses and determine what data is associated with each address.

1.26[8] HTML E-Mails Have More Functionality Than Text E-Mails. Text e-mails are an older protocol, and, as the name suggests, text only. There are no embedded pictures, tracking applets, or other advanced features. They are a simpler format, and almost every e-mail system can process and read them. However, their capabilities are limited.

HTML e-mails currently are the norm, as they permit imbedded pictures and graphics, a wider range of fonts, and tracking functions (such as tracking whether an e-mail was received or read, and how many times it was read). However, not all systems are able to handle all HTML formatting and tracking items. These can malfunction or cause the e-mail to be bounced by system filters.

If the e-mail is text only, the e-mail itself is likely to contain all the information there is on the e-mail. If the e-mail is HTML, however, additional tracking information is likely to be available.

Consider:

HTML e-mails can present a search challenge. Pictures and graphics can be embedded in HTML e-mails, and they may show words, but pictures and graphics cannot be searched. The search string will only search text. Since a computer search can't read words in an image, that image won't be "hit" and won't be returned by a computer search.



Strategic Point:

Counsel should consider whether this kind of image/graphic is an issue in the litigation in question. Even though it is not possible to search for text in an HTML e-mail, it is possible to search for the kinds of files or items that can be embedded as pictures and graphics. If those are located, the e-mails may need to be reviewed visually by review personnel, rather than handled electronically.

1.26[9] E-Mails Contain Important Metadata. Every e-mail system creates metadata to assist it in processing

e-mails. Some metadata fields are seen by the e-mail author and recipients, such as the ordinary routing information: the To, From, CC, BCC and Subject fields. Most of the metadata fields are never seen by the ordinary e-mail users. For example, as an e-mail enters the system, the local e-mail system usually assigns it a tracking number, so it can reference it and route it and find it and track "Replies" in the e-mail thread, etc. The user never needs this reference number. The e-mail program attaches the number to the e-mail for its own purposes, and simply doesn't show that kind of housekeeping function to the end recipients.

Strategic Points:



- There are many uses for e-mail metadata in e-discovery. First, metadata assists in de-duplicating. If e-mails can be matched, it is only necessary to look at one, decide what treatment it requires (privileged, non-privileged, confidential, other), and that treatment can be applied across all duplicates. It can assist in identifying e-mail threads--all e-mails in a conversation.

- Every e-mail system keeps slightly different sets of metadata information for the e-mails it is processing. Lotus Notes and Microsoft Exchange are the two most prevalent e-mail systems, and they keep different fields. The metadata fields available can also change between versions of a program. It is important to find what program and version were in use during a relevant time frame, and what e-mail metadata fields are available on that program/version.

Example:

An employee alleged that her former boyfriend, the company's CEO, had ordered her fired after she refused to have sex with him. It was undisputed that she had been fired five days after their last date. She settled the suit in 1995 for \$100,000. A key piece of evidence in that matter was a 1993 e-mail from her supervisor to the CEO confirming that he had terminated her at the latter's request. The supervisor denied that he had ever sent the e-mail. E-mail metadata, combined with cell phone records, showed the true story. A comparison of the time the e-mail was sent, and the supervisor's cell phone records, substantiated the supervisor's claim that he was traveling in his car at the precise time the e-mail was sent. The employee knew her supervisor's passwords, and had broken into his e-mail account and sent the e-mail herself. She was eventually charged and found guilty of forgery and falsification of evidence.

1.26[10] Some E-Mail Attachments Are Not Searchable. Just about any kind of ESI can be attached to an e-mail. *The key element to note here is that not all e-mail attachments can be searched.* If an e-mail attachment is a flat file--a picture file of some kind rather than text--it cannot be searched electronically. JPEGs, bitmaps, non-text PDFs, and TIFFs, are all common e-mail attachments. Searches will not penetrate them, and any text or other alphanumeric characters pictured in them will not be returned as "hits."

Strategic Points:



- Since some attachments can't be searched, counsel will need to set up other methods for locating and handling these items.

- Even though it is not possible to search for text in picture or graphics files, they can be located and identified for alternative handling. JPEG files end with the letters .JPG; bitmap files end with the letters .BMP; PDF files end with the term .PDF, etc. It is possible to search for those terms and locate the

attachments that the ordinary search term searches will not penetrate.

- Once they are located, what kind(s) are they? For example, if the resulting image files are TIFFs or PDFs of documents, they can probably be converted to searchable material by Optical Character Recognition (OCR). OCR will create text files of the imaged documents, and those can be searched by computer. If the resulting images are photographs, they will probably require eyes-on review by human reviewers.

1.26[11] Relationships Among E-Mail "Families" Should Be Preserved. The standard term for e-mail groups in the ESI industry is "families." The sending e-mail is the "parent" document, while e-mail attachments are "children." It is important when collecting or processing e-mails to preserve the "parent/child" relationships--to maintain an understanding of which documents are part of a "family" group, and which is the parent and which are the children.

Strategic Point:



Family relationships are important because context is important. For example, it is important to consider family relationships when conducting a privilege review. It may be that only one document in a "family" group is privileged. If this item is privileged, counsel must decide whether to designate the entire "family" as privileged, or redact this specific item and produce the rest of the family. When counsel locates privileged items through use of a computerized search string, it will be necessary to pull in the "hit" document's family unit so that the privileged item can be considered in its full context. For example, it may be that two documents do not look privileged in and of themselves. However, for example, the CEO may have attached them to an e-mail to outside counsel asking for legal advice about them. Usually, in this case, the entire communication--both e-mail and attachments--may be privileged. If counsel relied only upon the privilege "hits," only the parent e-mail would have been withheld, but when context of the entire group is considered, all of the communication might be withheld as privileged.



Cross Reference:

Discussion of privilege review, see *Ch. 9, Gathering and Producing Electronically Stored Information*, 9.36-9.46.



70 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

IV. UNDERSTANDING COMMONLY ENCOUNTERED TYPES OF COMPUTER-BASED ELECTRONICALLY
STORED INFORMATION AND THE ISSUES THEY PRESENT

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.27

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.27 Calendars and Related Functions.

For Outlook users, the contacts, calendar, notes and task functions are integrated with the e-mail function. It is possible, for example, to drag an e-mail into a calendar entry or a contacts entry. This type of integration is likely to become the norm with most commonly used applications.



71 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

IV. UNDERSTANDING COMMONLY ENCOUNTERED TYPES OF COMPUTER-BASED ELECTRONICALLY STORED INFORMATION AND THE ISSUES THEY PRESENT

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.28

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.28 Word Processing Programs and Other Document Applications.

1.28[1] Documents May Not Be All Text--Embedded and Referenced Items. Documents applications are no longer simply receptacles for text. Microsoft Word and other document-creation applications currently permit embedding of other file types. Therefore, a "document" may contain things such as pictures, video, animations, and sound files.

Document applications also permit referencing other documents available to the document owner. Referenced documents can be located anywhere the user's permissions permit them to reach. For example, a Word user can pull in an Excel file--and the Word document updates if the Excel file is changed.

This kind of integration causes various problems in e-discovery:

- If the document updates referenced items when it is opened, it may not be the same when discovery occurs as it was during the litigation's relevant time period.
- If the document is removed from its original context--the corporation's system--the link to a referenced document will be broken, and the referenced item may no longer appear properly in the envelope document. Both this and the preceding issue can lead to spoliation claims.
- If the items embedded in the document are photos, sound files, or other non-text items, they may contain information of interest in the litigation, but they cannot be searched using text strings. Furthermore, their presence is not apparent, because the envelope document looks like an ordinary text document--a Word document or WordPerfect document.



Warning:

These issues need to be taken into account, asked about, and handled in the document productions. They key point to remember is that even apparently textual items may not be entirely text, and will not be

entirely searchable through use of search strings.

1.28[2] Unprinted Document Text Items.

1.28[2][a] Some Elements in Electronic Documents Will Not Print. Many e-documents contain items that do not print out unless you change document defaults to order them to do so. If a production is made in native format, these items will not be a production issue--the original e-file will have all of the required information, and nothing is withheld.

However, issues may arise when the production is being made with TIFFs and PDFs, as those will not contain the unprinted information unless specific steps are taken to require it to print. Last but not least, these items need to be considered in the privilege and analytical review, and they are not readily apparent and may not be searchable through ordinary methods.

1.28[2][b] Author Comments and Annotations Normally Do Not Print. Spreadsheets and word processing documents permit the author to add comments that normally do not print out. They will not be visible unless the reviewer is examining the original e-file, and puts his or her mouse over the area where the annotation is located. Excel puts a small red spot in the upper right hand corner of cells with annotations. When the mouse pointer is placed on the red spot, the annotation pops up in a "bubble" for the user to see. These items contain relevant information and are an integral part of the e-document.



Warning:

If the files are simply converted to PDF or TIFF documents, this kind of unseen information is not included, as a TIFF or PDF file usually includes only the information that prints out. If counsel signs a certification stating that all relevant information has been produced, it may be faulty.



Strategic Point:

It is possible to change defaults and require that unseen annotations, comments, and other invisible materials all print out.

1.28[2][c] Redlining and Track Changes Will Not Print on Default Settings. Even if it is not showing on the screen, a word processing document may be tracking the changes being made. This is how a document permits the user to "undo" changes to go back a few steps. "Track changes" features may track only the last few changes, or it may track every change made since the document was created. These items do not print out unless commanded to do so.

Some systems also permit comparison of one document on the system against another, with the differences noted by "redlining." This too may not show on the ordinary screen, and yet is embedded in the document.

1.28[2][d] Auto-Date and Automatic Updating Functions May Change Documents. Many applications, including word processing and spreadsheet programs, permit the user to apply items that update automatically. The most common example of this is an auto-date. The date code updates every time the document is accessed/opened.

These functions present issues in native productions. If this item is produced in native format, the items will update when it is opened by the receiving party. If this is a prevalent feature, or if this presents a problem to receiving parties, it may be necessary to accompany the native files with TIFFs or PDFs.



Strategic Point:

This issue should be negotiated with opposing counsel as part of the discussion of formats, and an agreement reached.



Cross Reference:

Issues to be negotiated and discussed with opposing parties, see *Ch. 5, Initial Procedures--Notice, Document Preservation, Meeting and Conferring, and Case Management, 5.14-5.21*.

1.28[2][e] Opening or Printing File Changes File's Metadata. Like autocodes, the metadata relating to an item will change as soon as the item is opened, printed, or otherwise handled. For e-files, this includes items like the "last accessed" or "last printed" information. This presents a problem in native review and native productions, as the metadata will alter if the item is opened for review.



Strategic Point:

The metadata should be collected before the items are reviewed, so that it is the original metadata and no spoliation occurs. The stripped metadata can be loaded into a database that accompanies the native items, preserving the original information.



72 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

IV. UNDERSTANDING COMMONLY ENCOUNTERED TYPES OF COMPUTER-BASED ELECTRONICALLY STORED INFORMATION AND THE ISSUES THEY PRESENT

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.29

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.29 Computer Databases.

1.29[1] Databases Are Important in Litigation. Databases have been relevant to litigation for several decades. Early cases involving access to electronic data often involved databases. Because databases can be huge, and because litigants often do not understand the challenges associated with production of information from large databases, this can become contentious.

1.29[2] Definition and Types of Databases. A database is a standardized set of data or records that is stored in a computer and that may be searched or manipulated through the use of computer software. Databases also are sometimes referred to as "structured data systems."

The information in structured data systems takes its meaning from the structure in which it is organized. The data itself, outside of its context, is often useless. An example of a structured data system is enterprise accounting software.

Databases can vary substantially according to the level of complexity, size and formatting. Significant types of databases include:

- **Tables.** Tables created in a word processing program or a spreadsheet program are simple databases. Data is organized in rows and columns. Searching and retrieval is facilitated by the computer program use, e.g., Microsoft Word or Microsoft Excel.

Example:

An Excel spreadsheet can be used to organize financial information. For example, one could create an Excel file that listed payroll information such as payroll dates, amounts, department, and employee names.

- **Flat File Databases.** A flat file database contains information stored in predetermined fields. The fields can be searched and sorted, and one can generally perform Boolean searches as well.

Example:

Litigation support databases such as Concordance are flat file databases. For every record, or document, in a database, there are numerous fields including such fields as document identification or Bates number, Bates range, attachment range, date, or author. There are also fields that contain database information relating to each document, such as load date.

■ **Relational Databases.** Relational databases are more complex and facilitate the use of larger amounts of data for a variety of purposes. Relational databases can contain several files or collection of data. Each file typically will contain information in a table format, as is the case for a flat file database. The key feature of a relational database is that the same field (column) appears in several files (also known as "tables"). Because of this ability to link separate tables by reference to values in the common fields, one can search and also create reports from data in a database across all files as required to satisfy particular inquiries. Relational databases are created by the use of database software.

■ **Enterprise Databases.** Enterprise databases are sophisticated systems that allow the storage and retrieval of large volumes of data. These databases generally use database software that is customizable to some extent. The sheer volume of information and the use of specialized software means that discovery or relevant information from this type of database will present challenges.

■ **Reports.** Reports will often provide useable summaries of relevant information and can generally be customized to the needs of a case.

Example:

A corporation may use an Oracle database to track sales. In product liability litigation, a party might request information about sales in the United States for three years. For such sales, the database may contain thousands of fields or pieces of information, only some of which is relevant to the request. The challenge is to obtain the required information in a format that is useable. If the purpose of the request is to identify by name all purchasers of a product, the amount of data will be large and it may be necessary to deliver the data in a way that will allow it to be loaded into other database programs. On the other hand, if the purpose of the request is to obtain sales volume in units and dollars by state by year, the information may be easy to deliver in the form of a report. The report itself will not constitute a database or be produced in database format. Rather, it will be a document summarizing the data in the sales database.

**Strategic Point--Requesting Data Dictionaries:**

It may be useful to request data dictionaries for any databases of interest. This document, if one exists, will list all fields in the database and note the type of data to be found in each field.



73 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

IV. UNDERSTANDING COMMONLY ENCOUNTERED TYPES OF COMPUTER-BASED ELECTRONICALLY STORED INFORMATION AND THE ISSUES THEY PRESENT

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.30

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.30 Spreadsheets.

A spreadsheet is a table of rows and columns. The intersection of any given row and column is known as a "cell." The key useful feature of a spreadsheet is that the user can enter formulas into a cell that performs mathematical operations on numbers located in other cells.

Spreadsheets can be quite large, and documents produced by use of such software programs as Microsoft Excel will often require discussion regarding the form of production. If produced in TIFF or image format, they may not be readily comprehensible because formatting may have been lost:

- A spreadsheet in printed or TIFF form can be several thousand pages long.
- It may contain so many columns that it cannot fit within the confines of a single viewable or printable page.
- There may be hidden information that will only be viewable in the native version. For example, formulas may be embedded in a spreadsheet.

On the other hand, spreadsheets may contain simple alphabetized lists that are readily viewable in TIFF or image format.



Strategic Point:

Consider the types of information that may be contained in spreadsheets. If a matter involves extensive financial data, then it may be necessary to produce spreadsheets in native format. In other types of cases, it may be sufficient to produce documents in TIFF or image format, and reserve the right to request native format production for spreadsheets that require it. The information value of a spreadsheet derives from both the numbers themselves and from their positioning relative to each other. The TIFF conversion process often changes the manner in which that positioning is displayed, thus affecting the utility of the spreadsheet.

► **Cross Reference:**

Additional discussion of spreadsheets and TIFF format, see *Ch. 9, Gathering and Producing Electronically Stored Information*, 9.38.



74 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

IV. UNDERSTANDING COMMONLY ENCOUNTERED TYPES OF COMPUTER-BASED ELECTRONICALLY
STORED INFORMATION AND THE ISSUES THEY PRESENT

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.31

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.31 Presentation Software.

The use of presentation software, most notably Microsoft PowerPoint, has become widespread. These documents often reflect the agendas and discussions of meetings, and contain the following features:

- There is a field for speaker notes that may not appear if the presentations are produced in tiff or image format. Either native production or special processing may be required to obtain this data.
- Sophisticated presentations may contain embedded animations or video excerpts. TIFF or image production will not reveal this content in a meaningful way.



75 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

IV. UNDERSTANDING COMMONLY ENCOUNTERED TYPES OF COMPUTER-BASED ELECTRONICALLY STORED INFORMATION AND THE ISSUES THEY PRESENT

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.32

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.32 Websites.

1.32[1] Websites Can Be Important Sources of ESI. Websites have become increasingly important as they have become more robust. Much of the information that was once obtained by mail or by telephone contacts is now available on websites. Thus there has been increasing attention to the electronic discovery considerations for retention and production of information obtained via websites.

Because websites are constantly changing, it may be difficult to capture the content in a timely fashion. However, when the content of websites is an issue in litigation, it will be necessary for counsel to consider the ways in which website-based information can best be captured.

Example:

In *Arteria Prop. Pty Ltd. v. Universal Funding V.T.O., Inc. (DNJ 2008) 2008 US Dist LEXIS 77199*, the court held that plaintiff was entitled to spoliation sanctions due to defendant's failure to retain website information. The court stated that there was "no reason to treat websites differently than other electronic files."



Strategic Points:

- The full version of Adobe Acrobat contains a feature that can be used to create a PDF of a website, complete with clickable links to other pages in the website. It is only effective for smaller sites, but can be useful for documenting what a website shows at a given time.
- The nonprofit "Internet Archive" project stores versions of websites across time. The purpose is to create an archival library of the sites on the Internet during different time periods. It has a feature called the "wayback machine" that allows a user to enter the website's URL, and then see links to versions of

the website as they appeared on the Internet at different dates. This feature can be especially valuable for litigants who need to prove, for instance, what representations or terms and conditions were contained on a site at some point in the past [see www.archive.org].

1.32[2] Wikis. A wiki is a website that can be edited by multiple users by use of software designed to facilitate collaboration. Wiki is the name of the software used to create Wikipedia. The word "wiki" has taken on a generic meaning. There are other software programs that have a similar function.

1.32[3] Blogs. A blog is a type of website and is an shortened form of the word "weblog." It is an on-line journal that is maintained by one or more contributors, and it is accessible via the Internet.

Blogs may be started by anyone at any time. Blogs may be revised frequently or infrequently. They may be created and abandoned, or change in focus or purpose.

1.32[4] Intranets. An intranet is an internally maintained website that restricts access to authorized users. Often, entities maintain intranets accessible only by employees. They serve as a repository of frequently used information and may have significant value in e-discovery.

Example:

In *Fenster Family Patent Holdings, Inc. v. Siemens Medical Solutions USA, Inc.* (D Del 2005) 2005 US Dist LEXIS 20788 , the court denied a renewed motion for access to defendant's intranet; no new circumstances justified revisiting a previous ruling allowing the defendant to produce pages from the intranet rather than providing access to plaintiff.

1.32[5] Internet Browser Records. An Internet browser is a software application that allows users to have access to Internet-based websites. Microsoft's Internet Explorer and Mozilla Firefox are examples of popular browsers.

An Internet browser cache stores the web pages visited by a user of a particular machine on the machine's hard drive. The cache feature allows a user to quickly move back and forth between websites during a single internet session, and also facilitates ready access to previously visited websites during subsequent sessions. The information in the cache may be stored only temporarily, or it may be stored for some period of time. The cache resides on a local machine or server and is emptied periodically according to a schedule.

Visiting a website may also create other records on the computer. For example, a site may create a "cookie" on the computer--a file that identifies the computer and user to the website on later visits. The browser also may record the site in a browsing history record and/or an entry in a favorite sites file.

Examples:

- In *Gutman v. Klein* (EDNY 2008) 2008 US Dist LEXIS 92398 ; adopted by *Gutman v. Klein* (EDNY 2008) 2008 US Dist LEXIS 97709 , a court-appointed forensic expert examined the Internet cache of a laptop computer and found information that supported a claim of intentional spoliation.

- In *Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey* (ED Pa 2007) 2007 US Dist LEXIS 52544 , a court declined to sanction party that did not save web browser cache information when deletion was automatic and the party had no knowledge of potential relevance to unasserted claims.

1.32[6] Social Networking Sites. Social networking websites such as LinkedIn (geared towards professionals), MySpace, and Facebook allow people to post pictures and information about their lives to the world wide web for members of their social networks to view, and to communicate with each other through the sites. Facebook also allows

a user to comment on the status updates posted by another member of the user's network by posting comments ("writing") on a portion of the other member's page called "the wall." A member of a social networking site can join another member's individual network by either requesting an invitation from that individual or issuing the individual an invitation to join the member's network, depending upon the particular social networking website. The process of granting access to one's network has even entered the popular lexicon as "friending" an individual. Depending upon the privacy settings of an individual user, different content on the user's page can be viewed by the general public, all other members of the social network site, or only by individuals within the user's network of contacts, or "friends."

Many people share a significant amount of information about their daily lives on social network pages. Increasingly, the contents of these pages are relevant to litigation. The issue has arisen in sex discrimination lawsuits and cases alleging physical or emotional harm, among other contexts. The law in this area is still developing.

Examples:

- In a Title VII sex discrimination lawsuit, one of the asserted instances of discrimination was that the perpetrator recounted to plaintiff an off-color story with sexual overtones. In granting the defendant's motion for summary judgment, the court referenced the fact that the perpetrator had posted a reference to the story on his MySpace page, so that it would be available to both male and female members of his network. The court relied on the posting as evidence that the off-color story could not have been shared with the plaintiff *because of her sex*, and ruled that this type of "equal opportunity" harassment did not give rise to Title VII liability under existing Seventh Circuit precedent. Interestingly, the plaintiff herself had produced the information during discovery. She obtained it from a relative who was a member of MySpace and had access to the content of the perpetrator's site postings [*Treat v. Tom Kelley Buick Pontiac GMC, Inc.*, (ND Ind Apr. 30, 2010) 2010 US Dist. LEXIS 42811, *21- 23] .

- In a suit brought by the EEOC on behalf of a female claimant alleging sexual harassment in the workplace, a United States magistrate judge granted in part a defendant's motion to compel the EEOC to produce photos and other information the claimant had posted to her Facebook and MySpace pages. Because the EEOC was alleging that the claimant suffered psychological injuries as a result of the harassment, the court held that the photos were discoverable because the context of the pictures and the claimant's appearance might reveal the claimant's emotional and mental status. Similarly, the court held that the claimant's status updates, wall comments, groups joined, activity streams, postings, and messages that related to events that could reasonably be expected to produce a significant emotion, feeling or mental state, were relevant to the issue of whether the claimant suffered emotional injury and to the disputed issue of what caused any such injury [*Equal Employment Opportunity Commission v. Simply Storage Management, LLC* (SD Ind., May 11, 2010) Case No. 1:09-cv-01223-WTL-DML, "Order on Discovery Issues Raised During April 21 Conference," Document #46, 2010 US Dist. LEXIS 52766].

Cross Reference:

Discussion of ethical pitfalls in gathering evidence via social networking sites, see 3.09[3].

Discussion of social networking sites and the Federal Stored Communications Act, see 6.17[6].



76 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

IV. UNDERSTANDING COMMONLY ENCOUNTERED TYPES OF COMPUTER-BASED ELECTRONICALLY
STORED INFORMATION AND THE ISSUES THEY PRESENT

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.33

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.33 Voice Mail.

Digital voice mail systems have largely replaced analog systems. In digital voice systems, the messages are retained in a digital computer file. Moreover, many entities have unified messaging systems that deliver voicemail messages to a user's inbox.

Voice mails typically are stored as .wav files. Thus, while analog voice mails generally have not been the subject of litigation holds and document requests, digital voice mails messages can more easily be stored for long periods of time, and thus are producible, if relevant, in litigation. The trend in this area is affected by rulings in cases involving other types of audio records.



77 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

IV. UNDERSTANDING COMMONLY ENCOUNTERED TYPES OF COMPUTER-BASED ELECTRONICALLY
STORED INFORMATION AND THE ISSUES THEY PRESENT

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.34

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.34 Videos.

If relevant, video information will be subject to discovery.

Example:

In *Viacom Int'l Inc. v. YouTube Inc.* (SDNY 2008) 253 FRD 256, 261, a copyright infringement action, defendants were ordered to produce copies of "millions" of videos that were removed from the YouTube website.



78 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

IV. UNDERSTANDING COMMONLY ENCOUNTERED TYPES OF COMPUTER-BASED ELECTRONICALLY STORED INFORMATION AND THE ISSUES THEY PRESENT

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.35

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.35 Instant Messages.

Instant messages (IM) are short typed messages used by two or more people to communicate in a conversational, near simultaneous fashion. IM became popular in the late 1990s, with the advent of an AOL Instant Messenger (AIM). Whenever IM contacts, or "buddies," are online, a small window will indicate that fact to all IM contacts. Most systems are designed for the transmission of messages among buddies who are online at the same time. Newer applications allow messaging to buddies who are off line, thus increasing the similarities between IM and e-mail or voicemail.

IM may use web-based instant messaging products, or may be based on enterprise systems managed by an entity's IT staff. For enterprise-based systems, instant messages can be tracked and retained by the IT group.

Examples:

AOL Instant Messenger and Yahoo!IM are examples of consumer instant messaging programs. These messages cannot be preserved by a central IT group. Users may be able to activate IM archiving features and retain IM on their hard drives.

Consider:

The functionality of IM continues to improve. IM users can now share files via IM. Moreover, IM capabilities have expanded, and it is now common to use IM on a cellular telephone or other mobile device.

Strategic Point--Importance of IM in E-Discovery Is Increasing.



IM is increasingly important in litigation as it begins to be an accepted way of communication, to some extent replacing e-mail. If IM is used to communicate about topics that are relevant to a lawsuit, it may be necessary to preserve those messages and to consider producing them as a form of ESI. As was the case in the early days of e-mail, users often do not think that IM can result in a permanent record of very casual conversations.



79 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

V. UNDERSTANDING OTHER POTENTIAL SOURCES OF ELECTRONICALLY STORED INFORMATION
AND THE ISSUES THEY PRESENT

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.36

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.36 CHECKLIST: Understanding Other Potential Sources of Electronically Stored Information and the Issues They Present

- ☐ Understand backup processes and potential importance of backup media in e-discovery.

Discussion:

See 1.38

- ☐ Understand importance of hard drives and removable media.

Discussion:

See 1.39

- ☐ Understand operation of cellular phones and personal data assistants (PDAs) as a source of ESI.

Discussion:

See 1.40

- ☐ Understand potential value of third party customer account or financial records in e-discovery.

Discussion:

See 1.41

- ☐ Understand operation and potential value of social and professional networking sites in e-discovery.

Discussion:

See 1.42

- ☐ Understand how security data is potential source of ESI.

Discussion:

See 1.43



80 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

V. UNDERSTANDING OTHER POTENTIAL SOURCES OF ELECTRONICALLY STORED INFORMATION
AND THE ISSUES THEY PRESENT

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.37

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.37 Options and Strategies.

In addition to sources of ESI that reside on or typically are accessed via the owner's computer system, there are a number of sources of ESI that exist independently. One of the most important of these is "backup" media--data that has been moved off of a computer to a backup tape or other removable media, and stored separately, often off-site, for recovery in case of a severe system failure or similar disaster [see 1.38, 1.39]. Another area of ever-increasing importance is cellular phones and personal digital assistants (PDAs)--Palm Pilots, Blackberries, iPhones, and so on--that may hold relevant ESI [see 1.40]. The attorney should also consider third party records [see 1.41] and other potential sources as well.



81 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

V. UNDERSTANDING OTHER POTENTIAL SOURCES OF ELECTRONICALLY STORED INFORMATION AND THE ISSUES THEY PRESENT

*1-1 MB Practice Guide: CA E-Discovery and Evidence 1.38***AUTHOR:** Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin**1.38 Disaster Recovery Backup Media.**

1.38[1] Backup Systems Store Data for Recovery in Event of System Failure. A backup system allows a user to recover most stored information if there is a catastrophic failure of all or part of a computer system. Most organizations will have backup protocols, and many individuals back up their data periodically.

Backup media has been important in electronic discovery as they may be the only source of older data such as e-mails. There have been many discovery disputes about backup media because it can be expensive even to retain backup media, and very expensive to attempt to determine if there is unique, relevant data on that media.

Consider:

Case law relating to backup media generally involves backup tapes. As backup protocols change, identification of potentially relevant data on backup tapes is becoming possible. It may no longer be necessary to restore a number of tapes without knowing what might be on them. Moreover, backup tapes are being replaced by other backup protocols, such as disk to disk backup.

**Strategic Point:**

As a first step in e-discovery, it is often useful to ask for a physical inventory of backup media. Such an inventory will include information available by a physical inspection of the media, including such things as tape brand and label information. Consider asking for a header scan as well.

**Cross References:**

Form for demand for ESI, see *Ch. 6, Demanding Production of Electronically Stored Information in California Court*, 6.20.

1.38[2] Different Types of Backup Protocols Are Used. A backup protocol (policy and procedure governing the frequency and extent of backups) generally is selected to minimize time and expense in creating the backups, while

ensuring the ability to recover most data in the unlikely event of a catastrophic loss. The following backup protocols are most frequently encountered:

- **Full backup.** All data is backed up, with the exception of application software.
- **Differential backup.** A differential backup saves all files that have been changed since the last full backup. In order to recover lost data, it is necessary to restore the full backup and the most recent differential backup.
- **Incremental backup.** An incremental backup saves all files that have been changed since the last incremental backup. In order to recover lost data, it is necessary to restore the last full backup and all incremental backups created since the last full backup.

1.38[3] Backup Data Retention Periods Vary. In order to fulfill purpose as disaster recover tool, it is only necessary to save the last full backup and the subsequent incremental or differential backups. Nevertheless, many organizations retain backup media for a longer period.

1.38[4] Backups May Involve Tape Rotation. Tape rotation involves the reuse of a tape, writing over the existing information with new data. Tapes are generally rotated on a daily, weekly, or monthly basis.

Example:

Zubulake v. UBS Warburg (SDNY 2003) 217 FRD 309, 314 ("Zubulake I") describes a typical rotation schedule.

1.38[5] Testing and Sampling May Resolve Disputes About E-Discovery of Backups. Litigants have found it useful to process a selection of tapes when there is a dispute about the relevance or burden of producing data from backup tapes. Testing and sampling is specifically favored in the California Civil Discovery Act amendments [*CCP* § 2031.010(a)]. These techniques have been used successfully for a variety of purposes. For example, if a litigant claims that a data source will not contain relevant material, the parties may be able to agree to a sampling protocol that will allow that position to be proven or refuted. In addition, sampling or testing can be useful to in obtaining accurate cost estimates before embarking on a large ESI project. Parties can also use sampling or testing to fine tune a protocol for collection, processing and production.

Example:

In *Toshiba America Electronics Components v. Superior Court (2004) 124 CA4th 762, 21 CR3d 532*, the court ordered cost shifting for the translation of backup tapes, and urged the parties to meet and confer regarding sampling of the data on the tapes.



82 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

V. UNDERSTANDING OTHER POTENTIAL SOURCES OF ELECTRONICALLY STORED INFORMATION
AND THE ISSUES THEY PRESENT

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.39

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.39 Hard Drives and Removable Media Can Be Source of ESI.

This category includes external or internal hard drives, CDs, DVDs, flash or thumb drives, Zip drives, iPods and MP3 players. All of these media could contain relevant files. It is now possible to have a million documents on a thumb drive. These are freely available, and people routinely use them to transport and save data.



83 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

V. UNDERSTANDING OTHER POTENTIAL SOURCES OF ELECTRONICALLY STORED INFORMATION
AND THE ISSUES THEY PRESENT

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.40

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.40 Cell Phones and Personal Digital Assistants (PDAs).

1.40[1] Evolution of Technology Has Increased Importance As ESI Source. Cellular telephones are ubiquitous and have multiple functions. They are being replaced at the high end by PDAs, or Personal Data Assistants. PDAs include Palms, Blackberries, and iPhones. While these devices continue to serve as mobile telephones, many of them now have many of the functions of the standard laptop or desktop computer. Cell phones and PDAs have replaced personal computers, e-mail, appointment books, date books, address books, note pads, and watches.

This development has been facilitated by the appearance of full keyboards on the devices. The devices have been used by many as a primary method of written communication, including e-mail and text messaging, in addition to the traditional telephone function.

There can be important data on these devices, and data can be recovered from them. One important source of evidence may be text messages or "texts" that are transmitted between cell phones or between cell phones and e-mail addresses. Like e-mail and instant messaging, text messages may be an important source of evidence because many users are more spontaneous and less cautious in this form of communication.

Consider:

Many people have more than one cell phone.

1.40[2] Preservation and Recovery of Data Can Be Problematic. Hand-held devices may have limited memory, and data may become unavailable quickly. Users routinely delete data from cell phones, whereas there is a tendency for many to retain other ESI indefinitely.

The ability to recover data from cell phones varies widely depending on the device, including make and model as well as the service provider.



Strategic Points:

- For organizations, the IT department often will support employee PDAs. Many organizations will have a server dedicated to this task, such as a Blackberry server.
- For individuals, counsel can obtain copies of invoices from cell phone service providers. These invoices will often list numbers used for incoming and outgoing phone calls and text messages.

Consider:

Discovery of data from a hand-held device may seem more intrusive than from a personal computer. However, one can support an argument that the data is nevertheless discoverable with appropriate protection for private, non-relevant information, as is often done when data is collected from home computers.

**Cross Reference:**

Discussion of privacy issues in e-discovery, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferring, and Case Management Conference*, 5.19[7]; and see *Ch. 9, Gathering and Producing Electronically Stored Information*, 9.17.



84 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

V. UNDERSTANDING OTHER POTENTIAL SOURCES OF ELECTRONICALLY STORED INFORMATION
AND THE ISSUES THEY PRESENT

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.41

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.41 Third Party Customer Account or Financial Records May Contain Relevant ESI.

Many businesses now offer extensive online services to employees, clients, customers or consumers. For example, many banks now offer online access to bank accounts as well as the ability to pay bills electronically. In addition, many service providers such as telephone, cell phone, and credit card companies have electronic billing capabilities. It is possible for a consumer to have bills sent electronically to an online banking site and then to pay those bills electronically.

Documents such as bank records, brokerage statements, and call records may be readily available online, and represent an additional source of information. Indeed, some providers of consumer services may not make paper statements routinely available without a fee.



85 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

V. UNDERSTANDING OTHER POTENTIAL SOURCES OF ELECTRONICALLY STORED INFORMATION
AND THE ISSUES THEY PRESENT

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.42

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.42 Social or Professional Networking Sites May Contain Relevant ESI.

One of the most remarkable changes in communications involves the proliferation of social networking sites. Initially, primarily younger people were attracted to MySpace and Facebook, but now the appeal of these venues has spread to other segments of the population. In addition, professional networking sites such as LinkedIn have become popular. Moreover, entities such as corporations and nonprofits have launched Facebook pages to aide in marketing efforts. And more recently, Twitter has come onto the scene [see Boehring and Toal, "Social Networking Data Presents Challenges," New York Law Journal, July 1, 2009; see also "Are Social Networking Sites Discoverable?" Product Liability Law & Strategy, November 13, 2008]. The law in this expanding area is developing and full of open questions.

Strategic Points:



- Commentators have focused on the use of these sites by an employee using an employer-owned work station. In the context of employment litigation, such activity may be relevant to discipline regardless of the content.
- If an entity uses a social networking site for business purposes such as marketing, it becomes more difficult to argue that the data is not discoverable to the same extent that other online marketing efforts such as websites are discoverable.
- If relevant, attorneys will need to determine where the relevant data can be found, and how it may best be preserved. Typically, social networking data is stored on the servers of the site itself, and generally will not be found on a user's computer. It may be necessary to obtain technical guidance in order to preserve and obtain such data.



86 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

V. UNDERSTANDING OTHER POTENTIAL SOURCES OF ELECTRONICALLY STORED INFORMATION
AND THE ISSUES THEY PRESENT

1-1 MB Practice Guide: CA E-Discovery and Evidence 1.43

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

1.43 Security Data May Contain Relevant ESI.

Security data, including security camera data, electronic lock access records, and similar data may contain relevant and discoverable ESI. For example, many businesses now have electronic lock systems that respond to a user's code, fingerprint, or entry card. These systems typically maintain logs showing times of access that may be useful in litigation. Security or surveillance data may be stored for short periods of time and then recycled by businesses, so an attorney wanting production of surveillance information should act quickly to subpoena this ESI.

Example:

In *New Albertsons v. Sup. Ct. (2008) 168 CA4th 1403, 1429-1430, 86 CR3d 457*, a supermarket failed to preserve security videos in a slip and fall case. The negative inference issue sanction issued by the superior court was held to be unwarranted when the failure to preserve was due to the routine operation of the system, the video cameras were not directed towards the location of the plaintiff's fall, and the tapes were not necessary for plaintiffs to receive a fair trial.



87 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 1 Understanding Electronic Evidence

VI. GLOSSARY

1-1 MB Practice Guide: CA E-Discovery and Evidence

AUTHOR: Helen Marsh Diane E. Barry, Esq. Reviewed by Ernst Halperin

Appendix A: Glossary of Technical Terms Encountered in E-Discovery.

Active data: Information residing on the direct access storage media of computer systems, which is readily visible to the operating system and/or application software with which it was created and immediately accessible to users without undeletion, modification, or reconstruction (i.e., word processing and spreadsheet files, programs and files used by the computer's operating system). Another way of referring to active data is that it resides in the allocated file space on a computer. The computer's operating system can see it and retrieve it. For example, this term does not include deleted files that might reside on a hard drive. Those files cannot be seen by the operating system and will not be offered in menus for retrieval.

Algorithm: A mathematical set of steps designed to solve a problem or run instructions in a program. For example, an algorithm in a case management program would perform the function, "Check the filing date of the complaint in this matter, determine the date to file an answer, determine if the answer has been sent out and, if not, send e-mail to the attorney in charge of the case warning him of the impending date."A_and_footnotes(n1);vk n1

Allocated file space: The space on a computer where active data resides. In simple terms, allocated file space is that portion of a hard drive which the operating system has allocated for storage of files. It has items stored there; it knows what they are; it can retrieve them. These files are included in its indices for files it tracks and takes care of. Related terms: active data; unallocated file space; delete/deleted files.

Attachment: A record or file associated with another record for the purpose of storage or transfer. There may be multiple attachments associated with a single "parent" record. In ESI discovery, this term is most commonly used in reference to e-mails, where a file or files were associated with an e-mail for transfer and storage as a single message unit. It also crops up in paper productions when dealing with documents that have attachments or exhibits, such as a memo, report, or legal filing. For either, the industry standard is to refer to them as parent/child relationships, where the "parent" is the top document, and the attachments or exhibits are the "children." The "family" is the entire group--parents and children. The purpose of a discussion utilizing these terms is that counsel will wish to preserve the family relationship of such a group--counsel does not want to process e-mail data in a manner that separates the "parent" e-mail from its "child" attachments. Counsel also does not want a tracking database that doesn't track both the "parent"

memo and the "child" attachments as all being part of the same document. Rather, counsel will want a methodology that takes particular care to preserve or otherwise identify all such relationships.

Automated speech recognition/automated voice recognition (ASR/AVR): A program that will "translate" words spoken into a microphone connected to a computer into written text in a word processing program or perform a function in a database program. Commercial example: Dragon Naturally Speaking speech recognition software.

Back end/front end: Expressions used to describe programs or protocols relative to the user. A front-end program is one that interacts directly with the user, while a back-end program supports the front-end services, usually unseen by the user.

Bates numbering: A method of numbering legal documents for reference during discovery under which a unique identification number--which can be either numeric or alphanumeric--is assigned to each page of every document in question. Originally developed for paper documents, but now also used in e-discovery.

Blowback: Printing TIFF or PDF images onto paper.

Boolean search/query: Mathematical query language developed by English mathematician George Boole in the 19th century. Boolean searching of text is based on the underlying logic functions of various true/false statements. Common Boolean operators are "And," "Or" and "Not" commands, such as "Tom but not Jones" or "bankruptcy and trustee."

Boot/boot up: From the phrase "to lift oneself up by one's own bootstraps": the process whereby a computer automatically loads its startup software when it has been turned on.

Burn: To record or write data on a CD or DVD.

Cache: A collection of web page copies stored on a computer's hard disk or in its random-access memory (RAM). The browser accumulates these copies as the user browses the Web. When the user clicks a link or types a URL to fetch a particular web page for which the cache already contains a copy, the browser compares the cached copy to the original. If there have been no changes, the browser uses the cached copy rather than re-fetching the original, saving processing and download time [see *United States v. Parish* (9th Cir. 2002) 308 F3d 1025, 1030-1031 (contrasting downloading and caching of files); see also *United States v. Mohrbacher* (9th Cir. 1999) 182 F3d 1041, 1045-1048 (describing downloading)]. Related term: RAM/Random Access Memory.

Cache files: The Internet cache is an area to which the Internet browser automatically stores data to speed up future visits to the same websites. See *United States v. Parish* (9th Cir 2002) 308 F3d 1025, 1030, n 1031 (contrasting downloading and caching of files); see also *United States v. Mohrbacher* (9th Cir 1999) 182 F3d 1041, 1045-1048 (describing downloading).

CD-ROM: Compact disc read-only memory. CD-ROMs are a common way to store data from a computer, and many computers have CD-ROM drives for reading and/or writing CD-ROMs.

Chain of custody: All information on a file's travels from its original creation version to its final production version and ultimately to the version introduced in evidence at trial; a detailed account of the location of each document/file from the beginning of a project until the end. A sound chain of custody verifies that that information has not been altered either in the copying process or during analysis. If counsel cannot show the chain of custody, it may be difficult to disprove the argument that outside influences might have tampered with the data. A chain of custody failure--the mishandling of electronic evidence (even fully recovered files)--can cause a litigation defeat [see *Lorraine v. Markel* (D Md 2007) 241 FRD 534] .

Chain of evidence: The "sequencing" of the chain of evidence follows this order: identification and collection, analysis, storage, preservation, transportation, presentation in court, return to owner. The chain of evidence shows: who obtained the evidence, where and when the evidence was obtained, who secured the evidence, who had control or possession of the evidence, and what, if anything was done to the file and by whom, while it was in a particular custody stage.

Client/server network: A computer system functionally distributed across several nodes on a network, sometimes called a distributed application. The basic theory is that the various components of the system can be tailored to perform specific functions, hopefully for the good of the entire network. Client/server systems are also typified by a high degree of parallel processing across distributed nodes. Usually the clients are individual PCs connected to server(s) that act as central storehouses and "traffic cops" for information and applications.

Compare with file-sharing applications, in which all searches occur on the workstation, while the document database resides on the server. With client-server architecture, CPU-intensive processes (such as searching and indexing) are completed on the server, while image viewing and data entry occur on the client. File-sharing applications are easier to develop, but they tend to generate tremendous network data traffic in document imaging applications. They also expose the database to corruption through workstation interruptions. Client-server applications are harder to develop, but dramatically reduce network data traffic and insulate the database from workstation interruptions.A)_and_footnotes(n2);.vk n2

Cluster: The smallest unit of storage space required for computer data to be written to a drive, sometimes called an allocation unit.A)_and_footnotes(n3);.vk n3

Computer forensics: The use of specialized techniques for recovery, authentication and analysis of electronic data when a case involves issues relating to reconstruction of computer usage, examination of residual data (such as "deleted" data that has not been overwritten by the system), and authentication of data by technical analysis or explanation of technical features of data and computer usage. Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel.A)_and_footnotes(n4);.vk n4

Compression: Any method that reduces the amount of data necessary to transmit information from one point to another. Compression generally eliminates redundant information and/or predicts where changes will occur. "Lossless" compression techniques totally preserve the integrity of the input. "Lossy" methods disregard some of the originals. The ratio of the file sizes of a compressed file to an uncompressed file, e.g., with a 20:1 compression ratio, an uncompressed file of 1MB is compressed to 50KB.A)_and_footnotes(n5);.vk n5

Conceptual searching/querying: A process that maps relationships between each word and every other word in large sets of documents and then associates words based on the context in which they are used. Two techniques can be used to perform concept searches: the use of a manually constructed thesaurus that relates certain words to others; or semantic indexing, a fully automated methods to show associations among words based, in part, on statistical analysis of the occurrence of proximity of certain words to others.A)_and_footnotes(n6);.vk n6

Cookie: A small piece of information stored on a user's computer by web sites. When a user visits such a web site, the site asks the user's computer for permission to place one or more cookies on the user's hard drive. The purpose of the cookie is to identify the user, so the website can store information about them and match the information to the user if the user comes back to the site. For example, if the user returns to the site, the user's computer sends the site the cookie(s) that belong to it. The website now knows, for example, that this is the user who has the three items in their shopping cart; has visited the site at least once or twice a month for the last year, and is interested in Eastern philosophy books. A user can set the computer's cookie preferences to control how cookies are used and how much information they are willing to let web sites store on their hard drive. This is usually set through options in the browser, and/or

security programs such as firewalls. Related terms: Foreign Cookie/Third Party Cookie.A)_and_footnotes(n7);.vk n7

Database: A collection of information organized in such a way that a computer program can quickly select desired pieces of data. Often abbreviated DB or dB. A database can be thought of as an electronic filing system. Traditional databases are organized by fields, records, and files. A field is a single piece of information, a record is one complete set of fields, and a file is a collection of records. For example, a telephone book is analogous to a file. It contains a list of records, each of which consists of three fields: name, address, and telephone number.

A database can be *dynamic* (information updated regularly/constantly) or *static* (archive only--no updating).

The two most frequently used dB types are flat file and relational. A flat file stores data in a two dimensional display--for example, an Excel spreadsheet. A relational database organizes the data into tables that can be accessed and reassembled in multiple ways depending on the query being run--like a Rubik's Cube with the squares being twisted and reconfigured every time one queries the dataset.

Relational databases are typically set up to store related information in tables, and then link those tables together as necessary for the particular query needed. For example, a relational database may keep customer name, customer number, address, and phone numbers in a customer table, and data about an individual retail order (e.g., date, item, amount, customer number) in an orders table. To print an invoice listing orders, the database would combine information about the orders from a particular customer by linking the two tables together by the common customer number field.

Data extraction: The process of removing files and metadata from backup tapes or other compressed format, to an active file status.

Decryption: The process of unscrambling data that has been encrypted. Related terms: Cryptography, Encryption, Public-Key Cryptography.

Defragging/defragmenting: When a computer saves files, it breaks them into parts, and tucks the parts into various spaces on the computer's hard drive, wherever it has room. Defragging (slang for defragmenting) reorganizes the hard drive to make more usable space, and then gathers the various parts of files and stores them together. They parts are now in contiguous spaces rather than spread around on the hard drive. The process of defragging copies and moves file fragments, overwriting formerly unused space. This process is of interest in ESI discovery because the process usually overwrites part or all of deleted files.

Delete/deleted files: When one "deletes" a file using ordinary methods (such as the delete key on a keyboard, or right clicking with a mouse), the file is not eradicated from the computer's hard drive. Instead, the operating system simply takes note that the operator doesn't need the file anymore and erases the pointers to that file in its index. It "forgets" where that file is located. Put another way, it tells itself that that this file space is available for new storage--it can put a new file there. The space where the file is stored moves from allocated file space to unallocated file space. Depending on whether or not the computer actually uses that space to store another file, the deleted file may or may not be gone from the computer's hard drive, even weeks later. Or, it may exist as a file fragment (partially overwritten). Related terms: active data; allocated file space; unallocated file space; file fragments.

Digital certificate: A means of providing heightened security for the access of a website or a specific document. Digital certificates are electronic records that contain keys used to decrypt information, especially information sent over a public network such as the Internet. Digital certificates must be applied for and granted by a Certificate Authority (CA).A)_and_footnotes(n8);.vk n8

Digital Signature: A code created from both the data to be signed and the private key of the signer. The digital

signature will be unique for each piece of data signed. Even a single comma added to a message changes the digital signature for that message. Successful validation of a digital signature by appropriate software not only provides evidence that the person approved the transaction or message, but also provides evidence that the data did not change since it was "signed." Related terms: Public-Key Encryption.

Downloading: The act of manually storing a copy of a file or image located elsewhere on a computer network (storage media or Internet) to the user's hard drive or other personal storage for later retrieval. *See United States v. Parish (9th Cir 2002) 308 F3d 1025, 1030-1031* (contrasting downloading and caching of files); *see also United States v. Mohrbacher (9th Cir 1999) 182 F3d 1041, 1045-1048* (describing downloading).

Encryption: The process of scrambling information in a way that disguises its meaning, hopefully making it unintelligible/unusable by unintended recipients. Encrypted information can be decrypted only by someone who possesses the appropriate decryption key. Related terms: Cryptography, Decryption, Encryption, Public-Key Cryptography.

ESI: Electronically stored information--originally from the December 2006 amendments to the Federal Rules of Civil Procedure. This term is used in the Fed R Civ P to describe all electronic data discovery items. *Fed R Civ P 34(a)* states that ESI includes "writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained; translated if necessary, by respondent into reasonably usable form. ..." In California, the Electronic Discovery Act defines "electronically stored information" as "information that is stored in an electronic medium." The word "electronic" is defined as "relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities" [CCP § 2016(d), (e)]

File extensions: One or several letters at the end of a file name: .tif, .jpg, .pdf, .doc, .wpd, .pst, .nsf, .pif, .gif. File name extensions usually follow a period (dot) and indicate the type of information stored in the file. For example, in the filename letter.doc, the extension is ".doc," which indicates that the file is a word processing file. File extensions can streamline the process of locating data. For example, if one is looking for incriminating pictures stored on a computer, one might begin with the .gif and .jpg files.

File fragments: Most active data files are broken up into logical pieces and are stored separately in various locations on a single hard drive. When a file is "deleted," the computer operating system notes that all of the various places where the various file parts were stored are now available for overwriting with new data. If the OS makes use of that space and overwrites with a new data file, it may or may not overwrite all of the former data file's parts. Any remaining parts are referred to as file fragments, and if not overwritten, can be located through forensic examination of the target drive. Related terms: delete/deleted files; unallocated file space.

Firewall: A system intended to thwart unauthorized access to or from a private network that is often used to prevent unauthorized users from accessing a particular computer, or a private network of computers, when connected to the Internet.

Flash memory: A type of memory that retains data after power is removed. Flash memory operates both like memory and like a storage device. Flash memory is used in devices such as digital cameras, audio players, hand-held computers, cell phones, USB drives, and printers.

Floppy disk: An increasingly rare storage medium consisting of a thin magnetic film disk housed in a protective sleeve (largely replaced by CD-ROM and USB drives). A floppy disk is a small removable storage disk, also known as a diskette, generally available in two basic sizes, 3.5" and 5.25". The amount of data storage available on a floppy disk depends on the size and make, and can be anywhere from 360 kilobytes to 1.4 megabytes.

Foreign Cookie/Third Party Cookie: A cookie from that gets stored to a user's computer when the user visits a third

party website. This can occur when the site visited (the site visible to the user) is using or linking to content from a third site. The user may or may not be aware that they have shifted to content from a third party. (The link may be visible to the user or not.) Even though the user doesn't see that he or she has visited a third site, that third site can place a cookie on the user's hard drive. This kind of third party content can be anything, including images, text, or advertisements. Also known as "third-party cookie." Related terms: Cookie.

Forensic copy: When used in reference to a laptop or other stand alone workstation, the term means an exact bit-by-bit copy of the entire physical hard drive, including slack and unallocated space. Databases and servers are more complex. Industry standard for collection of forensic copies of servers usually takes active files only. If information from slack space or unallocated file space is wanted, it is necessary to request it specifically and discuss it with the collection team.

Forensically Sound: Forensics is the use of science or technology for the investigation and establishment of facts or evidence in a court of law. Preservation and acquisition of ESI evidence must be performed in a forensically sound manner; that is, in a manner that will permit the ESI to be entered into evidence in a court of law. This means that the ESI must be collected using reliable tools; using methods which are reliable and repeatable and generally accepted in the forensics scientific community; and that the resulting duplicate is a complete and accurate representation of the original. The methods used to capture the ESI must be documented at the time of capture, so that these facts can be proved when the evidence in question is offered into evidence. Related terms: Forensic Copy, Chain of Custody, Chain of Evidence.

Fuzzy searching/queriing: A full-text search procedure that looks for exact matches as well as similarities to the search criteria, in order to compensate for spelling or OCR errors.

FTP: File Transfer Protocol is the standard protocol or approach used to copy a file from one host to another using the Internet Protocol Suite known as TCP/IP [Transmission Control Protocol/Internet Protocol]. FTP is built on a client-server architecture and solves the problem of different end host configurations; for example, when the host is a UNIX system and the recipient is a Windows based server. FTP resolves the differences in operating systems, file names, and so on. FTP is useful when communicating between two very different systems, or when communicating across distances too remote to physically hand the data over, such as moving the data from a computer owned by a law firm in Fresno to the server of a coding vendor in India. FTP is not an instantaneous transfer, and it can take hours to move a bulk of data from one host to the target recipient.

GREP: GREP is shorthand for a search methodology that returns all instances of the target character string, regardless of word boundaries. For example, if a person uses a GREP protocol to search for the term "melon," it would return "watermelon" as well as "melons" and "melon." GREP was originally a command line text search utility written for Unix. The name is taken from the first letters of the instructions for the Unix text editor: Global/Regular Expression/Print. The default in Unix was for the search to be case sensitive (would not return Apple if you instructed it to look for "apple").

Hard disk/hard drive: The primary hardware that a computer uses to store information, typically magnetized media on rotating discs.

Hardware: All the physical mechanical and electrical parts of a computer.

Hash: An algorithm that creates a value to verify duplicate electronic documents. A hash mark serves as a digital thumbprint.

Hash value: A computed numerical value that represents a "digest" of the content of a file. Two documents will return the same hash value if and only if they are identical to the letter. The hash value is used as part of a digital signature and to compare document content in the de-duping process.A)_and_footnotes(n9);vk n9

Headers: E-mail term. E-mail headers are the lines at the top of an e-mail message that contain information used by the servers that process e-mail on the Internet. Their purpose is to permit routing and delivery of the message. An e-mail program normally shows only the standard To, From, Subject, and Date headers, but there is more. However, the header shows useful information, much like a trip itinerary does for a plane passenger. Who originated the message? How many stops did it make along its way to its ultimate destination, and where were they? This information travels with the e-mail in the header line. Caveat: As with ordinary travel, e-mails can be booked under a false name. It is common practice for spammers to at least partially falsify header information to hide the identity of the account that originated the e-mail.

Header scan: Searching the headers; looking for particular information in the headers.

Image key: The name of a file created when a page is scanned in a collection. For TIFFs, the image key is usually the Bates number of the paper document that was TIFFed.

IMAP: Internet Mail Access Protocol. IMAP and other server-based protocols make it easier to access e-mail from multiple locations rather than a single machine. When using IMAP, the e-mail system does not automatically download the entire e-mail to a user's local system. At first, it downloads only the message header the To, the From, the CC, the Subject, and a few other items. If the user opens the e-mail, the entire e-mail is then downloaded to the user's local system. The importance of this protocol to ESI discovery is that under IMAP, e-mail messages usually remain on the e-mail server even after they have been deleted from user's hard drive. In addition, when examining the user's system, if the user deleted it without opening it, the examiner will find only the header information in the wastebasket area or in the deleted files. There are protocols that bypass this protocol. For example, many users change the settings to synchronize their local system with the IMAP server in order to read and answer e-mails while not online.

Inactive data: No universally accepted single meaning, but can refer to active data that is not in use--data that is taking up room on the servers but should be moved over to archive. Sometimes also used to refer to data in slack space (that is, not in active areas) of the hard drive.

Intranet: A private or internal network that uses standard Internet protocols so it has the appearance of a Web site.

JPEG: Joint Photographic Experts Group. An image compression format used for storing color photographs and images.

LAN: Local area network. A LAN is a group of associated computers that share a common communications line and server within the same geographic area. Typically, LAN users share applications and data storage on the same server.

Legacy data/system: This term refers to antiquated, obsolete computer data and systems. Generally, it means that the data is in an outdated format, or that it resides on a storage system so antiquated or obsolete that the company no longer has the hardware or software required to access and view the data thus stored. Or, if the ancient equipment exists, it doesn't work. (Examples: accounting data tape from 10 years ago--the company has changed software twice times since then and no one knows where the hardware machine that ran it is located; a WordStar word processing document--software popular in the 1970s.) This term usually raises the question of why the client still has this data or system. There is likely a good argument that legacy data and systems should be classified as data that is not "reasonably accessible" [see CCP § 2031.060(c)-(e) (party seeking protective order must show data is not reasonably accessible)].

Litigation hold: The process at the outset of a matter required to halt a records retention or other destruction of information relevant to an ongoing or potential litigation or investigation. The process usually requires identifying, notifying, and counseling of relevant key players and document custodians to ensure timely preservation of all relevant information.

Lossless compression: A compression technique that does not lose any data in the compression process. Related terms: compression; lossy compression.

Lossy compression: Data compression in which actual information is lost during compression. Once decompressed and opened, the result is something less than was in the original file. Generally, the goal for lossy compressions is to pick something that is not observable to lose. Related terms: compression; lossless compression.

Metadata: The information that a computer OS creates in order to store, track, and access a particular computer file. Think of it like the library index cards of ancient years--it has basic information on the book so a person can identify it among the other books (title, author, publisher, blurb). Then the card lists where to find this particular book on the library shelves. Metadata tracks this kind of basic information on particular electronic files--when it was created, who created it, when it was last modified, where it stored, etc. The particular metadata fields available are different for different kind of files. For example, the metadata for an e-mail will list the date and time it was sent. A Microsoft Excel file is not sent, so the OS doesn't have "Sent" data for this kind of file. For e-mails, metadata can include: BCC, date received, opened status, undeliverable, etc. Metadata is of interest because it can be useful to understanding more about a particular document and its relevance to the case.

Mirroring/mirrored copy: A method of data backup that copies or "mirrors" each saved file on a hard disk onto a second hard disk.

Motherboard: The main circuit board in a computer. The motherboard has slots for and houses a variety of microchips, sockets, and plugs, and plays an integral part in connecting all of a computer's parts together.

Native format: A datafile/document in the format of the original application used to create the file.

Native production: A datafile/document produced in the format in which it was originally created.

NSF: A Lotus Notes e-mail archive file.

OCR: Optical character recognition. A method for scanning printed material and converting it into an electronic file, which can then be computer searched/queried. OCR recognizes only alphanumeric characters, not handwritten or other graphic material.

Operating system/OS: Software that directs the overall activity of a computer (e.g. MS-DOS, Windows, Linux).

OST file (.ost): An offline folder file in Microsoft Outlook. Offline folders make it possible for the user to work offline and then to synchronize changes with the Exchange server the next time they connect. The ability to work offline is useful in environments with limited or unreliable connectivity.

PDA: Personal digital assistant. Any small hand-held wireless device that provides computing and data storage abilities. Examples of PDAs include Palm Pilot, iPaq, and BlackBerry.

PDF: Portable Document Format. A proprietary format of Adobe Corporation, it has become a de facto standard for transmitting documents that the sender does not want to be altered and for transmitting documents to commercial printers and to the Web for online publishing. PDF captures formatting information from a variety of desktop publishing applications, making it possible to send formatted documents and have them appear on the recipient's monitor or printer as they were intended. Viewing requires Adobe Acrobat Reader, a free application distributed by Adobe Systems.

Phishing: A method of identity theft. "Phishing" consists of creating a look-alike trap website that seems to belong to a

legitimate company. The visitors are lured to the site, thinking they are buying something from, or providing information to, a legitimate business. Through these stratagems, the user is lured into submitting personal information or money/credit to the site. The criminals then use the personal information for their own purposes, or sell the information to other criminal parties.

Pixel: Abbreviation for picture element. Pronounced "PICK-sull." A pixel is the smallest element on a display screen. Images on a computer screen are made up of hundreds to thousands of pixels, and the screen's resolution is determined by the size, number, and closeness of the pixels.

POP: Post Office Protocol. POP is the oldest method of distributing e-mail through the Internet. Systems utilizing POP download the entire e-mail message to a user's local system when the user connects up. With the default settings, the e-mail is deleted from the mail server once it is downloaded, and the e-mail resides only on the user's local system. Related term: IMAP

PST: A Microsoft Outlook archive file. Can contain a compressed version of any or all of the Outlook utilities--e-mail, contacts, task list, journal, and so forth--depending on settings used by the person or entity who created the archive.

Public-Key Cryptography: A set of well-established techniques and standards that allow a person, an organization, or particular piece of hardware such as a server or router, to electronically verify its identity to third parties, or to sign and encrypt electronic data. Two pieces of computer data are involved: public keys and a private key. The public key is published as part of a certificate which associates that key with a particular identity. Data encrypted with the public key can be decrypted only with the private key.

EXAMPLE:

A wants B to send private information to A. B wants A to be the only one who can receive and use the information B is going to send. A issues B a public key and A keeps the private key. B uses the public key that A sent to encrypt the information B is going to send. Only A can decrypt this information after B encrypts it--only A's private key can decrypt the information encrypted with the public key A sent B.

RAM: Random access memory. Short-term memory used by a computer to temporarily store data for use by a computer program that is running. It may be possible to cause the computer program to store the contents of RAM into a more permanent storage location where it may be collected for litigation [see, e.g., *Columbia Pictures Indus. v. Bunnell* (CD Ca 2007) 245 FRD 443, 446-447 ; (CD Cal Aug 24, 2007) 2007 US Dist LEXIS 63620 (in copyright infringement action, court held that defendant must turn on logging feature of server in order to preserve records of Internet file requests)].

Records retention schedule: A plan for the management of records, listing types of records, and how long they should be kept. The purpose is to provide continuing authority to dispose of or transfer records to historical archives.

Residual data: Sometimes referred to as "ambient data"; refers to data that is not active on a computer system. Residual data includes:

- Data found on media free space;
- Data found in file slack space; and
- Data within files that has functionally been deleted in that it is not visible using the application with which the file was created, without use of undelete or special data recovery techniques.

ROM: Read only memory. Long-term memory whose contents can be accessed and read but cannot be changed.

Router: A piece of hardware that routes data from a local area network (LAN) to a phone line.

Sampling: The process of statistically testing data for the presence of relevant information. Items for test can be selected randomly, or at specified intervals.

Server: A computer on a network that contains data or applications shared by users of the network on their client PCs.

Slack space: A form of residual data. Data is stored in segments. If data doesn't fill an entire segment, the space left is slack space. In technical terms, slack space is the space on the hard disk from the end of the logical record information to the end of the physical disc record. Slack space can contain information that was deleted (soft-deleted) from the data record. It can contain information from old files that were previously stored at this location--since the new record didn't need all of the space, it didn't write over the entire old file, and left a fragment in the slack space. It can also contain metadata fragments and other information useful for forensic analysis of computer systems. Related term: residual data.

Source code: The computer program as it was actually written by the programmer. A compiler or assembler must translate the source code into an object code (machine language) that the computer can understand. Source code is written in a formal programming language (C++, Pascal, Basic, Unix, APL, etc.) and is then compiled automatically into object code or machine code or executed by an interpreter.

Spoliation: The deliberate or inadvertent modification, loss, or destruction of evidence by a party who has been put on notice of a duty to preserve, but has failed to take appropriate steps to preserve the potentially relevant evidence in their custody or control.

Spoofing: Digitally pretending to be someone else. For example, a person can pretend to have the email address jdoe@mozilla.com, or a computer can identify itself as a site called www.mozilla.com when it is not. Spoofing is one form of misrepresentation.

SQL: Structured Query Language. Pronounced "see-kwul." SQL is a standard programming language for getting information from and updating a database. Although SQL is a standard, many database products support SQL with proprietary extensions to the standard language.A)_and_footnotes(n10);vk n10

TIFF: Tagged Image File Format. This is the de facto standard for production of paper documents--8-bit color and grayscale. Originated in 1986 as a joint project of Microsoft and Aldus. Includes several types and groups that are compressed and uncompressed.

Unicode: Unicode is a data encoding standard that maps the characters and symbols used in various writing systems to a common definition so that a given character will always have the same binary representation. Prior to Unicode, different encoding standards, e.g., Latin 1, Windows Code Page 1251, each used the same binary codes to represent different characters. Unicode compliance comes into play primarily in foreign language matters, when ESI collections must be made in a Unicode-compliant manner so that language is preserved when moving the data from its original program into another one, for example, when moving e-mail from a foreign language e-mail system into a document review tool for search, review, and analysis. Microsoft Outlook systems that are newer than Outlook 97 store data by default as Unicode.

Unallocated file space: Space on a hard drive not currently in use by the computer for either active data or other storage. This is the space that the computer has available for storage of new files. However, that is not to say that unallocated file space is necessarily empty. For example, the computer's operating system can use unallocated file space for keeping temporary information it needs for the current session, but won't need thereafter. It can also be where deleted files exist. From the operating system's point of view, either there's nothing there, or there's nothing there it

needs to keep. Therefore, unallocated file space can be empty, or it can contain intact files, remnants of files, subdirectories, or temporary files that were created and then deleted by either a computer application, the operating system or the operator.

URL - Uniform Resource Locator: The standardized address that tells a browser how to locate a file or other resource across the Worldwide Web.

EXAMPLE:

www.lexis.com. Also known as an Internet address or Web address.

WAN: Wide area network. A network that connects computers in remote locations.

Wipe: The deliberate permanent deletion or overwriting of a piece of media in order to remove any trace of files or file fragments.

WYSIWYG: What you see is what you get (pronounced "wiz-ee-wig"). For data exports or printing, it refers to a system that allows the user to see onscreen exactly what will be printed out (example: the word processing programs that lets the viewer "preview" the printed document). For data inputs, it refers to a system that won't alter the data from the page or input format--no standardization of terms, no fixing of misspelled words, etc. Whatever is on the source document/file is what goes into the new system.

FOOTNOTES:

(n1)Footnote 1. Legal Electronic Document Institute, Basic Principles of Automated Litigation Support (2005).

(n2)Footnote 2. American Document Management, Glossary of Terms, <http://www.amdoc.com/glossary.shtml>.

(n3)Footnote 3. RSI, Glossary

(n4)Footnote 4. Kroll Ontrak, Glossary of terms: <http://www.krollontrack.com/glossaryterms>.

(n5)Footnote 5. American Document Management, Glossary of Terms, <http://www.amdoc.com/glossary.shtml>.

(n6)Footnote 6. Legal Electronic Document Institute, Basic Principles of Automated Litigation Support (2005).

(n7)Footnote 7. Ibis Consulting, Glossary (www.Ibisconsulting.com).

(n8)Footnote 8. Fios, E-Discovery Glossary. www.fios.com.

(n9)Footnote 9. Ibis Consulting, Glossary (www.Ibisconsulting.com)

(n10)Footnote 10. Legal Electronic Document Institute, Basic Principles of Automated Litigation Support (2005).



88 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 2 Governing Law in Electronic Discovery

1-2 MB Practice Guide: CA E-Discovery and Evidence 2.syn

§ 2.syn Synopsis to Chapter 2: Governing Law in Electronic Discovery

2.01 Scope.

2.02 Objective and Strategy.

2.03 Overview of Governing Law.

2.03[1] Discovery Act Governs All California Discovery.

2.03[2] Special Rules Apply to E-Discovery.

2.03[3] California Reported Case Law Is Relatively Sparse.

2.03[4] Federal Case Law Is Often Used As Source for Guidance.

2.03[5] Evidence Rules Govern Introduction of ESI.

2.04 Parties Must Initially Meet and Confer Regarding E-Discovery Issues.

2.05 Party May Seek Injunctive Relief to Preserve ESI.

2.06 Each Party May Demand Discovery of Electronically Stored Information.

2.06[1] Definition of Electronically Stored Information ("ESI").

2.06[2] Any Party May Demand Production of Electronically Stored Information.

2.06[3] Party Making Demand May Specify Form of Production.

2.06[4] Any Party May Demand Testing and Sampling.

2.07 Respondent May Object to Demand for Electronically Stored Information.

2.07[1] Responding Party May Object on Grounds That Source Is Not Reasonably Accessible.

2.07[2] Responding Party May Object to Specified Form of Production.

2.08 Statutory Rules Govern Production of Electronically Stored Information That Is Not Reasonably Accessible.

2.08[1] Respondent May Seek Protective Order.

2.08[2] Court May Allow Discovery on Showing of Good Cause.

2.08[3] Court May Allocate Expenses and Set Other Conditions.

2.09 Court Has Power to Limit Frequency and Extent of Discovery.

2.10 Statutory Rules Govern Form of Production.

2.10[1] Responding Party May Object to Form of Production.

2.10[2] Production in Ordinarily Maintained or Reasonably Usable Form Is Required Absent Agreement or Court Order.

2.10[3] Translation of Data Compilations May Be Required at Demanding Party's Expense.

2.11 Similar Statutory Rules Govern Subpoenas to Nonparties.

2.11[1] Parties Have Right to Subpoena Electronically Stored Information From Nonparty.

2.11[2] Rules Govern Form of Production by Nonparty.

2.11[3] Nonparty May Oppose Production.

2.11[4] Court May Require Production on Showing of Good Cause.

2.11[5] Court May Allocate Expenses and Set Other Conditions.

2.11[6] Court Has Power to Limit Frequency and Extent of Discovery From Nonparty.

2.11[7] Statute Protects Nonparties Against Undue Burden and Expense.

2.11[8] Parties to Litigation Outside of California May Obtain ESI Held in California by Nonparty.

2.12 Statutory and Case Law Govern Inadvertent Production of Privileged Electronically Stored Information.

2.12[1] Responding Party May Retrieve Inadvertently Disclosed Privileged Information.

2.12[2] Counsel Who Receives Inadvertently Disclosed Privileged Information Must Follow Specified Return Procedure.

2.13 Parties May Be Sanctioned for Spoliation of Evidence.

2.13[1] Parties Have a Duty to Preserve Evidence.

2.13[2] Sanctions May Not Be Imposed for Good Faith Loss or Destruction of Electronically Stored Evidence.

2.14 Comparison of Federal and California Law on Electronic Discovery.

2.14[1] Differences Exist Between Federal and California E-Discovery Law.

2.14[2] Scope of Discovery May Be Broader Under California Law.

2.14[3] California Does Not Require Mandatory Initial Disclosure.

2.14[4] Chart Comparing Federal and California E-Discovery Law.

2.15 Different Forums Have Different Electronic Discovery Rules.

2.16 Courts Generally Apply Local Discovery Rules.



89 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 2 Governing Law in Electronic Discovery

I. STRATEGY

1-2 MB Practice Guide: CA E-Discovery and Evidence 2.01

2.01 Scope.

This chapter provides an overview of the framework of California statutes and rules applicable to the discovery of electronically stored information, including the following:

- The California Electronic Discovery Act and the federal rules governing electronic discovery [see 2.03].
- Meeting and conferring regarding electronic discovery [see 2.04].
- Demanding electronically stored information [see 2.06].
- Responding to a demand for electronically stored information [see 2.07].
- Production of electronically stored information that is not reasonably accessible [see 2.08].
- Limits on the frequency and extent of discovery of electronically stored information [see 2.09].
- The form of production of electronically stored information [see 2.10].
- Subpoenas for electronically stored information [see 2.11].
- Inadvertent production of privileged electronically stored information [see 2.12].
- Sanctions for spoliation of evidence [see 2.13].

The procedures and issues arising under each of the above topics are discussed in greater detail in other chapters of the publication.

In addition, this chapter covers:

- Comparison of California and federal law on electronic discovery [see 2.14].

- Determining what law on electronic discovery is applicable [*see* 2.15-2.16].



90 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 2 Governing Law in Electronic Discovery

I. STRATEGY

1-2 MB Practice Guide: CA E-Discovery and Evidence 2.02

2.02 Objective and Strategy.

The law governing electronic discovery varies from jurisdiction to jurisdiction. Some jurisdictions have adopted comprehensive electronic discovery rules, while others rely on general discovery principles. Counsel in cases likely to involve the discovery of electronically stored information should determine what rules apply and familiarize themselves with the different issues they are likely to encounter.

Counsel trying cases in California state courts need to be aware of the California rules governing e-discovery, both in the context of the overall framework of California civil procedure and discovery law, and the specific context of the particular case. Counsel who are familiar with the federal rules governing e-discovery need to understand the differences and similarities between e-discovery in federal and state courts. Counsel who are not yet familiar with California's 2009 discovery rules need to understand what those rules do, how they change the former law, and how they are likely to affect e-discovery practices in California state court litigation.



91 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 2 Governing Law in Electronic Discovery

II. UNDERSTANDING THE FRAMEWORK OF CALIFORNIA ELECTRONIC DISCOVERY LAW

1-2 MB Practice Guide: CA E-Discovery and Evidence 2.03

2.03 Overview of Governing Law.

2.03[1] Discovery Act Governs All California Discovery. Electronic discovery in California, like all discovery, is governed generally by the Civil Discovery Act [*CCP* §§ 2016.010-2036.050] and applicable California Rules of Court. The rules and procedures applicable to civil discovery in general, including the implementing rules of court, apply to electronic discovery [*see Cal Rules Ct, Rules 3.1000, 3.1020, 3.1025, 3.1030*].

2.03[2] Special Rules Apply to E-Discovery. In 2009, the California legislature passed the Electronic Discovery Act [Stats. 2009 ch. 5 (effective June 29, 2009)] to address the problems created by application of the general Discovery Act rules to the specific issues that typically arise in e-discovery. *Section 23 of the Electronic Discovery Act* states that the Act is an urgency statute within the meaning of Article IV of the California Constitution and "shall go into immediate effect" [Stats. 2009, ch. 5, § 23]. The Electronic Discovery Act is modeled in part on federal rules governing e-discovery that took effect December 1, 2006, adapted to California civil procedure [*see Fed R Civ P, Rules 16(b)(3)(B)(iii), (iv), 26(b)(2)(B), (b)(5), (f)(3)(c), 34(b)(1)(C), (b)(2)(D), (b)(2)(E), 37(e)*].

Consider:

Although the California statutes did not specifically reference discovery of electronically stored evidence prior to passage of the Electronic Discovery Act in 2009, for many years before the passage of the Electronic Discovery Act California courts allowed discovery of electronically stored information, and often its admission into evidence, under the general discovery statutes then in effect [*see, e.g., People v. Lugashi* (1988) 205 CA3d 632, 640, 252 CR 434 (allowing admission of bank computer records); *R.S. Creative v. Creative Cotton* (1999) 75 CA4th 486, 89 CR2d 353 (terminating sanctions for actions including spoliation of evidence on computers)].

Case management requirements regarding discovery of electronically stored information are set out in *Cal Rules Ct, Rules 3.724(8), 3.728(13)*.

2.03[3] California Reported Case Law Is Relatively Sparse. Only a handful of California cases decided before the passage of the 2009 Electronic Discovery Act directly address electronic discovery issues. Therefore, lawyers and courts must continue to apply general discovery law principles to electronic discovery until a body of case law develops under the Electronic Discovery Act.

2.03[4] Federal Case Law Is Often Used As Source for Guidance. Because of the newness of the California electronic discovery statutes, and the infrequency with which e-discovery issues were considered in published California court opinions under the prior law, federal and out-of-state authority is more important in e-discovery cases than in other California cases dealing with more generic discovery issues. In particular, federal court decisions under the Federal Rules of Civil Procedure are important sources for guidance on the treatment of e-discovery issues.

The Federal Rules of Civil Procedure were revised in 2006 to deal specifically with e-discovery issues [*see Fed R Civ P, Rules 16(b)(3)(B)(iii), (iv), 26(b)(2)(B), (b)(5), (f), 34, 37*]. This was before most states (including California) had established their own rules governing e-discovery in state proceedings. As a result, state courts throughout the United States have often looked to federal judicial decisions--primarily in the federal district courts--for guidance on how to deal with similar e-discovery issues under state law.

Because of the larger body of federal law on electronic discovery, this publication cites federal authority when there is no available California authority. Many electronic discovery issues are resolved at the federal district court level in unreported decisions. Because those decisions are citable under federal rules and are often the only source of guidance on how courts have resolved e-discovery issues, they are included in this publication.

2.03[5] Evidence Rules Govern Introduction of ESI. The introduction of electronically stored evidence in court is governed by rules of evidence.



Cross Reference:

Admission of electronic evidence at trial, see Ch. 15, Admissibility of Electronic Evidence at Trial.



92 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 2 Governing Law in Electronic Discovery

II. UNDERSTANDING THE FRAMEWORK OF CALIFORNIA ELECTRONIC DISCOVERY LAW

1-2 MB Practice Guide: CA E-Discovery and Evidence 2.04

2.04 Parties Must Initially Meet and Confer Regarding E-Discovery Issues.

Unless the court orders another time period, no later than 30 calendar days before the date set for the initial case management conference, the parties must meet and confer, in person or by telephone, to consider the following [*Cal Rules of Ct, Rule 3.724(8)*]:

- Any issues relating to the preservation of discoverable electronically stored information.
- The form or forms in which information will be produced.
- The time within which the information will be produced.
- The scope of discovery of the information.
- The method for asserting or preserving claims of privilege or attorney work product, including whether such claims may be asserted after production.
- The method for asserting or preserving the confidentiality, privacy, trade secrets, or proprietary status of information relating to a party or person not a party to the civil proceedings.
- How the cost of production of electronically stored information is to be allocated among the parties.
- Any other issues relating to the discovery of electronically stored information, including developing a proposed plan relating to the discovery of the information.

The court's case management order may include orders relating to the discovery of electronically stored information [*see Cal Rules of Ct, Rule 3.728(13)*].



Cross Reference:

Discussion of Rule 3.724(8) meet and confer procedure, see Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferring, and Case Management Conference.



93 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 2 Governing Law in Electronic Discovery

II. UNDERSTANDING THE FRAMEWORK OF CALIFORNIA ELECTRONIC DISCOVERY LAW

1-2 MB Practice Guide: CA E-Discovery and Evidence 2.05

2.05 Party May Seek Injunctive Relief to Preserve ESI.

In rare instances when delay would likely mean loss of ESI, a party may seek a court order preserving ESI and/or providing for the copying of ESI in order to prevent loss of necessary ESI [*Dodge, Warren & Peters Ins. Services, Inc. v. Riley (2003) 105 CA4th 1414, 1417-1418, 130 CR2d 385*] .

Cross Reference:

Ch. 7, Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery.



94 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 2 Governing Law in Electronic Discovery

II. UNDERSTANDING THE FRAMEWORK OF CALIFORNIA ELECTRONIC DISCOVERY LAW

1-2 MB Practice Guide: CA E-Discovery and Evidence 2.06

2.06 Each Party May Demand Discovery of Electronically Stored Information.

2.06[1] Definition of Electronically Stored Information ("ESI"). The Electronic Discovery Act defines "electronically stored information" (frequently referred to as "ESI") as "information that is stored in an electronic medium" [see *CCP § 2016.020(e)*]. "Electronic" is defined as "relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities" [see *CCP § 2016.020(d)*].

Cross Reference:

Discussion of types of electronically stored information, see Ch. 1, Understanding Electronic Evidence.

2.06[2] Any Party May Demand Production of Electronically Stored Information. Any party may demand that any other party produce electronically stored information for inspecting, copying, testing or sampling [*CCP § 2031.010(a), (e)*].

Cross Reference:

Discussion of requesting production of electronically stored information, see Ch. 6.

2.06[3] Party Making Demand May Specify Form of Production. A party demanding the production of electronically stored information may specify the form or forms in which each type of electronically stored information is to be produced [*CCP § 2031.030(a)(2)*].

Cross Reference:

Discussion of requesting production of electronically stored information, see 6.01-6.12.

2.06[4] Any Party May Demand Testing and Sampling. The traditional means of obtaining information from documents under the Civil Discovery Act was through inspection and copying. As amended in 2009 to allow for the discovery of electronically stored information, the Civil Discovery Act allows a party to *test* and *sample* electronically stored information, in addition to inspecting and copying it [*CCP § 2031.010(a), (e)*].



95 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 2 Governing Law in Electronic Discovery

II. UNDERSTANDING THE FRAMEWORK OF CALIFORNIA ELECTRONIC DISCOVERY LAW

1-2 MB Practice Guide: CA E-Discovery and Evidence 2.07

2.07 Respondent May Object to Demand for Electronically Stored Information.

2.07[1] Responding Party May Object on Grounds That Source Is Not Reasonably Accessible. In its response to a demand for discovery of electronically stored information, a party may object on the grounds that the electronically stored information is from a source that is not reasonably accessible because of undue burden or expense. The responding party must identify in its response the types or categories of sources of electronically stored information that it asserts are not reasonably accessible. By objecting and identifying the type or category of sources that are not reasonably accessible, the responding party preserves its objections relating to that electronically stored information [CCP § 2031.210(d)].

2.07[2] Responding Party May Object to Specified Form of Production. If the responding party objects to the specified form for producing electronically stored information, it may state in its response the form in which it intends to produce each type of information [CCP § 2031.280(c)].



Cross Reference:

Discussion of responding to demand for electronically stored information, see Ch. 8, Responding to Electronic Discovery Demands in California Court.



96 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 2 Governing Law in Electronic Discovery

II. UNDERSTANDING THE FRAMEWORK OF CALIFORNIA ELECTRONIC DISCOVERY LAW

1-2 MB Practice Guide: CA E-Discovery and Evidence 2.08

2.08 Statutory Rules Govern Production of Electronically Stored Information That Is Not Reasonably Accessible.

2.08[1] Respondent May Seek Protective Order. A party from whom electronically stored information is sought may seek a protective order on the basis that the information is from a source that is not reasonably accessible because of undue burden or expense. The party seeking the protective order bears the burden of demonstrating that the information is from a source that is not reasonably accessible [CCP § 2031.060(c)].



Cross References:

Discussion of opposing request for production of electronically stored information, see Ch. 10, Opposing Demands for Production of Electronic Evidence in California Court

Discussion of seeking protective order, see Ch. 11, Seeking or Opposing Protective Order.

2.08[2] Court May Allow Discovery on Showing of Good Cause. Even if the responding party establishes that the information is from a source that is not reasonably accessible because of undue burden or expense, the court may nonetheless order discovery if the demanding party shows good cause, subject to limitations on frequency and extent [CCP § 2031.060(d)].

2.08[3] Court May Allocate Expenses and Set Other Conditions. A court that orders discovery of electronically stored information from a source that is not reasonably accessible may set conditions for the discovery of the electronically stored information, including allocation of the expense of discovery [CCP § 2031.060(e)].



97 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 2 Governing Law in Electronic Discovery

II. UNDERSTANDING THE FRAMEWORK OF CALIFORNIA ELECTRONIC DISCOVERY LAW

1-2 MB Practice Guide: CA E-Discovery and Evidence 2.09

2.09 Court Has Power to Limit Frequency and Extent of Discovery.

The court must limit the frequency or extent of discovery of electronically stored information, even from a source that is reasonably accessible, if the court determines that any of the following conditions exists [*CCP* §§ 2031.060(f), 2031.310(g)]:

- It is possible to obtain the information from some other source that is more convenient, less burdensome, or less expensive.
- The discovery sought is unreasonably cumulative or duplicative.
- The party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought.
- The likely burden or expense of the proposed discovery outweighs the likely benefit, taking into account the amount in controversy, the resources of the parties, the importance of the issues in the litigation, and the importance of the requested discovery in resolving the issues.

Cross Reference:

Discussion of limiting frequency or extent of discovery, see Ch. 10.



98 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 2 Governing Law in Electronic Discovery

II. UNDERSTANDING THE FRAMEWORK OF CALIFORNIA ELECTRONIC DISCOVERY LAW

1-2 MB Practice Guide: CA E-Discovery and Evidence 2.10

2.10 Statutory Rules Govern Form of Production.

2.10[1] Responding Party May Object to Form of Production. Although the party demanding the production of electronically stored information may specify the form of production for each type of electronically stored information [CCP § 2031.030(a)(2)], the responding party may object to the specified form and may state in its response the form in which it intends to produce each type of information [CCP § 2031.280(c)].



Strategic Point--Responding Party:

If the responding party objects to the requested form of discovery and provides the discovery in another form, the receiving party may seek a court order compelling production in the desired format [see Ch. 12, Seeking or Opposing Motion to Compel; see, e.g., *Bray & Gillespie Mgmt. LLC v. Lexington Ins. Co.* (M.D. Fla. Mar. 4, 2009) 2009 US Dist LEXIS 21250 (sanctions for producing in TIFF when metadata was requested); *L.H. v. Schwarzenegger* (C.D. Cal. 2008) 2008 US Dist LEXIS 86829 (sanctions for producing non-sortable PDFs); *3M Co. v. Kanbar* (N.D. Cal. June 14, 2007) US Dist LEXIS 45232 (defendant who printed 170 boxes of documents must produce again in electronic form)].

2.10[2] Production in Ordinarily Maintained or Reasonably Usable Form Is Required Absent Agreement or Court Order. Unless the parties otherwise agree or the court otherwise orders, 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 or forms in which it is ordinarily maintained or in a form that is reasonably usable. A party need not produce the same electronically stored information in more than one form [CCP § 2031.280(d)].

2.10[3] Translation of Data Compilations May Be Required at Demanding Party's Expense. If necessary, the responding party at the reasonable expense of the demanding party must use detection devices to translate any data compilations included in the demand into reasonably usable form [CCP § 2031.280(e)].



Cross Reference:

Discussion of form of production of electronically stored information, see Ch. 9, Gathering and Producing Electronically Stored Information.



99 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 2 Governing Law in Electronic Discovery

II. UNDERSTANDING THE FRAMEWORK OF CALIFORNIA ELECTRONIC DISCOVERY LAW

1-2 MB Practice Guide: CA E-Discovery and Evidence 2.11

2.11 Similar Statutory Rules Govern Subpoenas to Nonparties.

2.11[1] Parties Have Right to Subpoena Electronically Stored Information From Nonparty. The rules governing subpoenas of electronically stored information from nonparties are similar to those governing discovery of electronically stored information from parties. A party may serve a subpoena on a nonparty allowing the party to inspect, copy, test, or sample electronically stored information [CCP § 1985.8(a)(1)].

2.11[2] Rules Govern Form of Production by Nonparty. The rules governing production of electronically stored information by nonparties pursuant to subpoena are similar to those governing production by parties. A party serving a subpoena requiring production of electronically stored information may specify the form or forms in which each type of information is to be produced [CCP § 1985.8(b)]. If a subpoena requiring production of electronically stored information does not specify a form or forms for producing a type of electronically stored information, the person subpoenaed may produce the information in the form or forms in which it is ordinarily maintained or in a form that is reasonably usable [CCP § 1985.8(c)(1)]. A subpoenaed person need not produce the same electronically stored information in more than one form [CCP § 1985.8(c)(2)].

If necessary, the subpoenaed person, *at the reasonable expense of the subpoenaing party*, must use detection devices to translate any data compilations included in the subpoena into reasonably usable form [CCP § 1985.8(g)].

2.11[3] Nonparty May Oppose Production. A subpoenaed person may oppose the production, inspection, copying, testing, or sampling of electronically stored information on the basis that the information is from a source that is not reasonably accessible because of undue burden or expense. The subpoenaed person bears the burden of demonstrating that the information is from a source that is not reasonably accessible [CCP § 1985.8(d)].

2.11[4] Court May Require Production on Showing of Good Cause. Even if the responding party establishes that the information is from a source that is not reasonably accessible because of undue burden or expense, the court may nonetheless order production of the electronically stored information if the demanding party shows good cause, subject to limitations on frequency and extent [CCP § 1985.8(e)].

2.11[5] Court May Allocate Expenses and Set Other Conditions. The court may set conditions for the production of the electronically stored information, including allocation of the expense of discovery [CCP § 1985.8(f)].

2.11[6] Court Has Power to Limit Frequency and Extent of Discovery From Nonparty. The court must limit the frequency or extent of discovery of electronically stored information, even from a source that is reasonably accessible, if the court determines that any of the following conditions exists [*CCP § 1985.8(h)*]:

- It is possible to obtain the information from some other source that is more convenient, less burdensome, or less expensive.
- The discovery sought is unreasonably cumulative or duplicative.
- The party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought.
- The likely burden or expense of the proposed discovery outweighs the likely benefit, taking into account the amount in controversy, the resources of the parties, the importance of the issues in the litigation, and the importance of the requested discovery in resolving the issues.

2.11[7] Statute Protects Nonparties Against Undue Burden and Expense. The Civil Discovery Act provides a nonparty served with a subpoena for electronically stored information additional protections against undue burden and expense:

- First, a party serving a subpoena requiring the production of electronically stored information must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena [*CCP § 1985.8(j)*].
- Second, a court order requiring compliance with a subpoena for electronically stored information must protect a person who is neither a party nor a party's officer from undue burden or expense resulting from compliance subpoena [*CCP § 1985.8(k)*].

Federal practice is similar, although the Federal Rules of Civil Procedure do not have a statute analogous to *CCP § 1985.8(k)*.

Example:

Plaintiff, a social gaming company, sued unknown "Doe" defendants for infringing plaintiff's trademarks by selling online gaming chips that could be used in plaintiff's games. Plaintiff then moved for a court order permitting it to conduct discovery from four web hosting sites, ostensibly in order to discover the identities of the defendants. Plaintiff sought to obtain "all billing and account records (including all Internet domain names), server logs, website content, contact information, transaction histories and correspondence for the persons or entities that have purchased services from [pertinent hosting site name] in connection with the Internet domain name ... " The court limited the scope of the proposed subpoenas to "all documents necessary to obtain the name, current and permanent addresses, telephone numbers, and valid e-mail addresses of the owner(s)" [*Zynga Game Networks, Inc. v. John Does 1-5 (ND CA, January 1, 2010) 2010 U.S. Dist. LEXIS 9390, *8 & *9*].

Distinguish:

Note that these additional protections are not extended to *parties* from whom ESI is sought.



Cross Reference:

Discussion of discovery of electronically stored information from nonparty, see Ch. 6.

2.11[8] Parties to Litigation Outside of California May Obtain ESI Held in California by Nonparty. The

Interstate and International Depositions and Discovery Act [*CCP* § 2029.100 *et seq.*] governs depositions in California for out-of-state actions. The Act is California's version of the Uniform Interstate Depositions and Discovery Act [*see CCP* § 2029.700]. The Act provides one set of uniform procedures to be followed in all California courts. The procedures enable out-of-state litigants to obtain documents, including electronically stored information, from nonparties located in California [*see CCP* § 2029.200, § *CCP* 2029.350]. The Act clarifies that a request for the issuance of a subpoena does not constitute an appearance in a California court [*see CCP* § 2029.300(a)].

**Cross References:**

Discussion of subpoenas that may be issued by the clerk of the court or by counsel, *see* 6.17[2].

Detailed discussion of Interstate and International Depositions and Discovery Act, *see California Forms of Pleading and Practice*, Ch. 193, *Discovery: Depositions*, §§ 193.130 *et seq.*, 193.280 *et seq.* (forms); Ch. 535, *Subpoena*, §§ 535.21B, 535.85 (form).



100 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 2 Governing Law in Electronic Discovery

II. UNDERSTANDING THE FRAMEWORK OF CALIFORNIA ELECTRONIC DISCOVERY LAW

*1-2 MB Practice Guide: CA E-Discovery and Evidence 2.12***2.12 Statutory and Case Law Govern Inadvertent Production of Privileged Electronically Stored Information.**

2.12[1] Responding Party May Retrieve Inadvertently Disclosed Privileged Information. If a party discovers that privileged (or attorney work product protected) electronically stored information was produced in discovery, the party making the claim may notify any party that received the information of the privilege claim and the basis for the claim [CCP § 2031.285(a), (d)(1)]. After being notified, the receiving party must immediately sequester the information and either return it (and any copies) or within 30 days present the information to the court conditionally under seal for a determination of the claim [CCP § 2031.285(b)]. Until resolution, the receiving party must preserve the information and keep it confidential and is precluded from using or disclosing the information [CCP § 2031.285(c), (d)(2)]. If a party disclosed the information before being notified of the privilege claim, the party must immediately take reasonable steps to retrieve the information [CCP § 2031.285(c)(2)].

Compare--Applicability to Subpoenas:

These rules apply also to subpoenas [CCP § 1985.8(i)].

 Cross Reference:

"Clawback" rule governing recovery of privileged information, see 3.14.

2.12[2] Counsel Who Receives Inadvertently Disclosed Privileged Information Must Follow Specified Return Procedure. CCP § 2031.285 [see 2.12[1]] does not impose any affirmative obligations on counsel who receive inadvertent productions of privileged information until notified by producing counsel. However, the California Supreme Court has held that when a lawyer receives materials subject to attorney-client privilege, and it is reasonably apparent that they were inadvertently disclosed by another attorney, the recipient attorney should refrain from examining them any more than is essential to ascertain whether they are privileged, and should then immediately notify the sender. The parties should resolve the situation by agreement or with court assistance, if necessary. An attorney who violates this rule by using the privileged information faces disqualification [*Rico v. Mitsubishi Motors Corp.* (2007) 42 C4th 807, 68 CR3d 758, 171 P3d 1092] .

 Cross References:

Discussion of ethical duties of recipient of inadvertently disclosed privileged information, see Ch. 3.



101 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 2 Governing Law in Electronic Discovery

II. UNDERSTANDING THE FRAMEWORK OF CALIFORNIA ELECTRONIC DISCOVERY LAW

1-2 MB Practice Guide: CA E-Discovery and Evidence 2.13

2.13 Parties May Be Sanctioned for Spoliation of Evidence.

2.13[1] Parties Have a Duty to Preserve Evidence. Destroying evidence in anticipation of a discovery request or in response to a discovery request constitutes a misuse of discovery in violation of *CCP § 2023.010* [*Cedars-Sinai Med. Ctr. v. Superior Court* (1998) 18 *C4th* 1, 12, 74 *CR2d* 248, 954 *P2d* 511 ; *R.S. Creative, Inc. v. Creative Cotton, Ltd.* (1999) 75 *CA4th* 486, 495, 89 *CR2d* 353 (affirming order resulting in terminating sanctions for forging contract and destroying evidence by use of computers in violation of stipulation not to use the computers pending examination by expert)]. *CCP § 2023.030* authorizes a court to impose a variety of different sanctions for misuse of the discovery process, including monetary sanctions, issue sanctions, evidence sanctions, terminating sanctions and contempt sanctions.

Cross References:

Discussion of document preservation obligations, see Ch. 5.

Discussion of sanctions for spoliation of evidence, see *13.03-13.10*.

2.13[2] Sanctions May Not Be Imposed for Good Faith Loss or Destruction of Electronically Stored Evidence. Absent exceptional circumstances, a court may not impose sanctions on a subpoenaed person or any attorney of a subpoenaed person for failure to provide electronically stored information that has been lost, damaged, altered, or overwritten as the result of the routine, good faith operation of an electronic information system [*CCP § 2031.060(i)*; see also *CCP §§ 1985.8(l), 2031.300(d), 2031.310(j)*].

Cross References:

Discussion of sanctions, see Ch. 13, Seeking or Opposing Sanctions for Noncompliance.



102 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 2 Governing Law in Electronic Discovery
 III. COMPARISON OF FEDERAL AND CALIFORNIA LAW

1-2 MB Practice Guide: CA E-Discovery and Evidence 2.14

2.14 Comparison of Federal and California Law on Electronic Discovery.

2.14[1] Differences Exist Between Federal and California E-Discovery Law. Because California's electronic discovery rules are modeled in part on the 2006 amendments to the Federal Rules of Civil Procedure, the differences between the two are relatively minor. Nevertheless, practitioners who are familiar with the federal rules and procedures need to be aware of the differences between California and federal law. Some of those differences are discussed below.

2.14[2] Scope of Discovery May Be Broader Under California Law. The scope of allowable discovery under California's rules is differently described and perhaps broader than the scope allowed in the Federal Rules. The Federal Rules allow parties to obtain discovery "regarding any nonprivileged matter that is *relevant to any party's claim or defense*" [*Fed R Civ P 26(b)(1)* (emphasis added)]. California's rule, by contrast, provides that any party may obtain discovery "regarding any matter, not privileged, that is *relevant to the subject matter* involved in the pending action" [*CCP § 2017.010* (emphasis added)].

2.14[3] California Does Not Require Mandatory Initial Disclosure. Early in litigation, *Fed R Civ P 26(a)(1)* requires parties to disclose evidence to each other without waiting for a discovery request. Among the items that must be provided, or alternatively described by category and location, is electronically stored information that a party may use to support its claims or defenses [*Fed R Civ P 26(a)(1)(A)(ii)*]. California does not have such a requirement.

2.14[4] Chart Comparing Federal and California E-Discovery Law. The following chart compares the federal and California e-discovery rules.

California	Federal	
Scope of Discovery	California's scope of discovery is broader than that found in the Federal Rules: CCP § 2017.010 provides that any party may obtain discovery regarding any matter, not privileged, that is <i>relevant to the subject matter</i> involved in the pending action.	Parties may obtain discovery regarding any nonprivileged matter that is <i>relevant to any party's claim or defense</i> [<i>Fed R Civ P 26(b)(1)</i>].
Definition of Electronically	CCP § 2016.020(e) defines "elec-	The Federal Rules do not pre-

1-2 MB Practice Guide: CA E-Discovery and Evidence 2.14

Stored Information	tronically stored information" as "information that is stored in an electronic medium," and CCP § 2016.020(d) defines "electronic" as "relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities."	cisely define "electronically stored information." Fed R Civ P 34(a) covers information "stored in any medium," which is intended to encompass future developments in computer technology [Fed R Civ P 34(a) advisory committee's note to 2006 amendment].
Initial Disclosures	California does not require initial disclosures.	Fed R Civ P 26(a)(1) requires initial disclosures among parties, including provision or description by category and location of electronically stored information [Fed R Civ P 26(a)(1)(A)(ii)].
Meet and Confer Requirements	Cal Rules Ct, Rule 3.724(8) provides that unless the court orders another time period, no later than 30 calendar days before the date set for the initial case management conference, the parties must meet and confer regarding electronically stored information. Rule 3.724(8) describes a number of topics to be discussed. The court's case management order may include orders relating to the discovery of electronically stored information [see Cal Rules Ct, Rule 3.728(13)].	Fed R Civ P 26(f) requires parties to confer as soon as practicable, and in any event at least 21 days before a scheduling conference is held or a scheduling order is due under Rule 16(b). The parties must develop a proposed discovery plan stating the parties' views and proposals on any issues about disclosure or discovery of electronically stored information, including the form or forms in which it should be produced. After receiving the parties' report, the court must enter a scheduling order, which may include provisions for disclosure or discovery of electronically stored information [Fed R Civ P 16(b)(5)].
Testing and Sampling	CCP § 2031.010(a), (e) allow a party to test and sample electronically stored information in addition to inspecting and copying it.	Fed R Civ P 34(a)(1) is substantially the same
Information That Is Not Reasonably Accessible	A responding party may object to a request for production of information that is not reasonably accessible due to undue burden or expense, and/or seek a protective order [CCP § 2031.210(d), CCP § 2031.060(c)]. The responding party bears the burden of demonstrating that the information is from a source that is not reasonably access-	Fed R Civ P 26(b)(2)(B) provides that a party need not produce electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. To obtain discovery, the party seeking discovery must bring a motion to compel. As in California, the producing party

1-2 MB Practice Guide: CA E-Discovery and Evidence 2.14

	ible.	bears the burden of making the required showing [Fed R Civ P 26(b)(2)(B)].
Discovery Allowed on Showing of Good Cause	Even if the responding party establishes that the information is from a source that is not reasonably accessible because of undue burden or expense, the court may nonetheless order discovery if the demanding party shows good cause, subject to limitations on frequency and extent [CCP § 2031.060(d)].	Fed R Civ P 26(b)(2)(B) is substantially the same
Allocation of Expense	A court that orders discovery of electronically stored information from a source that is not reasonably accessible may set conditions for the discovery of the electronically stored information, including allocation of the expense of discovery [CCP § 2031.060(e)].	Fed R Civ P 26(b)(2)(B) provides that the court may specify conditions for the discovery. Federal courts have relied on this provision to allocate the expense of discovery.
Limits on Frequency or Extent of Discovery	The court must limit the frequency or extent of discovery of electronically stored information, even from a source that is reasonably accessible, if the court determines that any of the following conditions exists [CCP §§ 2031.060(f), 2031.310(g)]: ■ It is possible to obtain the information from some other source that is more convenient, less burdensome, or less expensive. ■ The discovery sought is unreasonably cumulative or duplicative. ■ The party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought. ■ The likely burden or expense of the proposed discovery outweighs the likely benefit, taking into account the amount in controversy, the resources of the parties, the importance of the issues in the litigation, and the importance of the requested discovery in resolving the issues.	Fed R Civ P 26(b)(2)(C) is substantially the same
Form of Production	CCP § 2031.030(a) allows the de-	Fed R Civ P 34(b) is substan-

	manding party to specify the form of production. CCP §2031.280(c) allows the responding party to object to the specified form and state in its response the form in which it intends to produce each type of information. CCP § 2031.280(d)(1) provides that if no form is specified, the responding party must produce the information in the form or forms in which it is ordinarily maintained or in a form that is reasonably usable. CCP § 2031.280(d)(2) provides that a party need not produce the same electronically stored information in more than one form.	tially the same.
Subpoenas	CCP § 1985.8 provides that a party serving a subpoena requiring the production of electronically stored information must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. A court order requiring compliance with a subpoena for electronically stored information must protect a person who is neither a party nor a party's officer from undue burden or expense resulting from compliance subpoena [CCP § 1985.8(j), (k)].	Fed R Civ P. 45(c)(1) is substantially the same
Inadvertently Produced Privileged Material	CCP § 2031.285 allows a party who inadvertently produces privileged (or attorney work product protected) electronically stored information to notify any party that received the information of the privilege claim. After being notified, the receiving party must immediately sequester the information and either return it (and any copies) or within 30 days present the information to the court conditionally under seal for a determination of the claim. Until resolution, the receiving party must preserve the information and keep it confidential, and is precluded from using or disclosing the information.	Fed R Civ P 26(b)(5)(B) is substantially the same.
Safe Harbor	CCP § 2031.060(i) provides a safe	Fed R Civ P 37(e) is substan-

harbor from sanctions for failure to provide electronically stored information that has been lost, damaged, altered, or overwritten as the result of the routine, good faith operation of an electronic information system. tially the same.



103 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 2 Governing Law in Electronic Discovery
IV. DETERMINING WHAT LAW IS APPLICABLE

1-2 MB Practice Guide: CA E-Discovery and Evidence 2.15

2.15 Different Forums Have Different Electronic Discovery Rules.

The law applicable to electronic discovery varies significantly among different forums. Federal courts were the first to develop comprehensive rules for electronic discovery with the 2006 amendments to the Federal Rules of Civil Procedure. Among state courts, some follow the federal rules, others have their own rules, and still others have no specific rules for electronic discovery and proceed under general state discovery law.



Strategic Point:

The federal and California rules for electronic discovery are sufficiently similar that they are not likely to be a factor in determining the forum in which to file an action.



Cross Reference:

Discussion of problems arising out of electronic discovery in foreign jurisdictions sanctions, see Ch. 14, Discovery of Electronically Stored Information Residing in Foreign Jurisdictions.



104 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 2 Governing Law in Electronic Discovery
IV. DETERMINING WHAT LAW IS APPLICABLE

1-2 MB Practice Guide: CA E-Discovery and Evidence 2.16

2.16 Courts Generally Apply Local Discovery Rules.

In general, courts apply their own discovery rules, even when they are bound by choice-of-law rules or a contractual choice-of-law provision to apply the substantive law of another forum [see *Hambrecht & Quist Venture Partners v. Am. Medical Int'l* (1995) 38 CA4th 1532, 1542, 46 CR2d 33]. Thus, electronic discovery in cases filed in California courts is governed by California's Electronic Discovery Act.

➤ **Cross References:**

Discussion of choice-of-law rules and contractual choice-of-law provisions, see *Matthew Bender(R) Practice Guide: California Contract Litigation*, 1.04-1.07.

Electronic discovery in cases filed in federal district is governed by the Federal Rules. This is true in both federal question cases and diversity cases, in which district courts apply state substantive law but federal rules of procedure [see *Erie R.R. Co. v. Tompkins* (1938) 304 US 64, 78-79, 58 S Ct 817, 82 L Ed 1188].

➤ **Cross References:**

Discussion of diversity jurisdiction, see *Matthew Bender(R) Practice Guide: Federal Pretrial Civil Procedure in California*, 2.09A-2.25; *Matthew Bender(R) Practice Guide: California Contract Litigation*, 1.22.



105 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

1-3 MB Practice Guide: CA E-Discovery and Evidence 3.syn

AUTHOR: Diane E. Barry, Esq.

§ 3.syn Synopsis to Chapter 3: Ethical Issues for Attorneys in E-Discovery

3.01 Scope.

3.02 Objective and Strategy.

3.03 CHECKLIST: Understanding Electronic Discovery Duties Owed to Clients.

3.04 Clients Bear Ultimate Responsibility to Preserve and Produce All Relevant Electronically Stored Records.

3.05 Attorneys' Duties to Clients Regarding Electronic Discovery Obligations.

3.05[1] Attorneys Have Duty to Explain Discovery to Clients.

3.05[2] Attorneys Have Duty to Be Actively Involved in or Monitor E-Discovery Collections.

3.05[3] Attorneys Must Have Reasonable Understanding of Client's Electronically Stored Information and Computer Systems.

3.05[4] Attorneys Have Duty to Assist and Monitor Litigation Holds.

3.06 Attorneys' Responsibilities for Client Electronic Discovery Responses.

3.06[1] Attorneys Have Duty to Conduct Reasonable Investigation of Foundation for Electronic Discovery Responses and Representations.

3.06[2] Late or Incomplete Electronic Discovery Responses Are Sanctionable.

3.06[3] Responsibility for Client Electronic Discovery Misconduct.

3.06[3][a] Attorney Is Not Responsible for Client Misconduct Not Known to Attorney.

3.06[3][b] Attorney Bears Responsibility for Client Misconduct Known or Assisted by Counsel.

3.06[3][c] Bases for Supporting Award of Sanctions Against Attorney.

3.07 CHECKLIST: Understanding Electronic Discovery Duties Owed to Courts and Opposing Counsel.

3.08 Attorneys Must Meet and Confer in Good Faith on Electronic Discovery Issues.

3.08[1] Attorneys Must Arrange to Meet and Confer.

3.08[2] Good Faith Conduct Requires Preparation.

3.08[3] Good Faith Conduct Requires Notice to Opposing Counsel That Discovery of Electronically Stored Information Will Likely Be Sought.

3.09 Attorneys Must Have Good Faith Basis for Electronic Discovery Representations Made to Court and Opposing Counsel.

3.09[1] Discovery Response Certifications and Court Filings.

3.09[2] Oral Communications and Correspondence.

3.09[3] Communications Via Social Networking Sites.

3.10 Attorneys Must Refrain From Discovery-Related Obstructionist Tactics.

3.10[1] Running Up Electronic Discovery Costs Is Improper.

3.10[2] Demanding Unnecessary Electronic Discovery Is Improper.

3.10[3] Negligence or Lack of Basic Knowledge Regarding Electronic Discovery Requirements Constitutes Incompetence.

3.11 CHECKLIST: Understanding Electronic Discovery Privilege Waiver Issues.

3.12 Options and Strategy When Material Sought in Electronic Discovery May Be Privileged.

3.13 California Attorney-Client Privilege and Attorney Work Product Protection.

3.13[1] Attorney-Client Privilege.

3.13[2] Attorney Work Product Protection.

3.13[3] Privileges Are Strictly Construed.

3.13[4] Privileges May Be Waived.

3.13[4][a] Waiver Through Voluntary Disclosure.

3.13[4][b] Compelled Disclosure Does Not Waive Privilege.

3.13[4][c] Failure to Object Manifests Consent.

3.13[4][d] Inadvertent Disclosure Does Not Manifest Consent.

3.14 Inadvertent Disclosure Does Not Constitute Waiver Under CCP § 2031.285 Clawback Rule.

3.14[1] Clawback Agreement Defined.

3.14[2] Clawback Rule Applies Only to Inadvertent Production of Electronically Stored Information.

3.14[3] Clawback Rule Does Not Create New Rights.

3.14[4] Clawback Rule May Be Modified by Parties.

3.14[5] Clawback Rule Does Not Decide Substantive Privilege Issues.

3.14[6] Clawback Rule Creates Framework for Producing Party to Reclaim Inadvertently Produced Materials.

3.14[6][a] Actions Are Specified From Perspective of Producing Party.

3.14[6][b] Notice to Receiving Party.

3.14[6][c] Contents of Notice.

3.14[6][d] Receiving Party Must Take Reasonable Steps to Sequester Identified Items.

3.14[6][e] Receiving Party Has 30 Days to Challenge Privilege Classification.

3.15 Ethical Obligations of Attorney Receiving Inadvertently Produced Privileged Electronically Stored Evidence.

3.15[1] CCP § 2031.285 Leaves Untouched Attorney's Pre-Existing Obligations.

3.15[2] Attorney's Obligations Are Ethical Rather Than Statutory.

3.15[3] Attorney's Ethical Obligations Arise As Soon As It Is Reasonably Apparent That Evidence Is Privileged.

3.15[4] Attorney Should Quarantine Potentially Privileged Items.

3.15[5] Attorney's Ethical Obligation to Notify Producing Counsel.

3.15[6] Attorney's Obligation to Settle Privilege Issues.

3.16 Privilege Issues That May Arise As Result of Using Computer Technology for Privilege Review.

3.16[1] Waiver Concerns.

3.16[2] Search Methodology.

3.16[3] Participant Qualifications.

3.16[4] Documentation and Proof.

3.17 Role of Federal Rule 502 in State Court Matters Involving Attorney-Client Privilege and Work Product.

3.17[1] Overview of Federal Rule 502 Concerns Effect of Attorney-Client and Work Product Privileges.

3.17[2] Effect of Federal Rule 502 on State Court Proceedings.

3.17[3] Federal Rule 502 Applies in Limited Circumstances.

3.18 CHECKLIST: Attorney's Ethical Duties Regarding E-Discovery Under the California Code of Professional Conduct.

3.19 Options and Strategy.

3.20 Remedies and Sanctions in Rules of Professional Conduct Are Not Exclusive.

3.21 Attorneys Must Act Competently When Performing Legal Services.

3.22 Attorneys Must Protect Client's Confidential Information From Disclosure.

3.23 Clawback Provision.

3.24 Notice to Receiving Counsel Regarding Inadvertent Production of Privileged Electronically Stored Information.

Diane E. Barry, Esq. n*

FOOTNOTES:

(n5)Footnote *. Diane E. Barry, Esq. is the Director of Discovery Strategy & Management at International Litigation Services, Inc. Diane's practice focuses on ESI discovery under state and federal rules of civil procedure, and complex litigation discovery planning and management. Diane assists clients in planning and preparing for ESI discovery conferences and court appearances, as well as preparation for specialized discovery such as IT custodian depositions, key player and IT interviews. In addition, Diane has significant expertise in utilizing technology to improve results in privilege and relevance review. Diane earned her A.B. degree from Vassar College and her J.D. degree, cum laude, from the Boston University School of Law. She also holds a professional certification in Data Warehousing from U.C. Berkeley.



106 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

I. STRATEGY

1-3 MB Practice Guide: CA E-Discovery and Evidence 3.01

AUTHOR: Diane E. Barry, Esq.

3.01 Scope.

This chapter covers ethical issues for attorneys particular to e-discovery matters, including:

- E-discovery-related ethical obligations and strategies [see 3.02].
- E-discovery duties owed to clients [see 3.04-3.06].
- E-discovery duties owed to courts and opposing counsel [see 3.07-3.10; Form: see 3.24].
- E-discovery privilege waiver issues [see 3.11-3.17; Form: see 3.23].
- Sanctions for misuse of discovery, including e-discovery [see 3.20].
- Attorney's e-discovery duties under the California Rules of Professional Conduct [see 3.17-3.22].

Core Statutes and Rules:

CCP §§ 2023.020, 2023.030, 2031.285; B&P Code §§ 6068, 6103; Evid Code §§ 912-920, 954, Cal Rules Ct, Rule 3.724; Cal Rules Prof Conduct, Rules 1-120, 3-100, 3-110, 5-200, 5-220.



107 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

I. STRATEGY

1-3 MB Practice Guide: CA E-Discovery and Evidence 3.02

AUTHOR: Diane E. Barry, Esq.

3.02 Objective and Strategy.

A litigating attorney faces a multitude of ethical issues and obligations, imposed by statute, case law, and rules of professional conduct. E-discovery is particularly rife with potential ethical pitfalls. This chapter provides broad ethical guidance for the e-discovery process, alerting counsel to commonly encountered ethical issues and providing strategies to resolve these issues.

Most of the ethical missteps common to e-discovery are the result of the attorney's discomfort with technology and client communications. For example, counsel is required to meet and confer with clients no later than 30 calendar days before the date set for the initial case management conference [see *Cal Rules Ct, Rule 3.724*]. Counsel facing the e-discovery process therefore must have a pointed technical discussion with the clients, early in the process, about their computer systems and available data evidence. If the information elicited is not accurate, or is not uncovered in a timely manner, misinformation will be communicated to opposing counsel and to the court or discovery referee. These actions may result in sanctions, other disciplinary actions, or malpractice claims against the attorney.

Strategic Points:



- Because e-discovery requires particular technical expertise, counsel should consider retaining a technical expert early in the proceeding. The better practice is to engage and consult with a technical expert before the meetings with clients that will be necessary to prepare for the "meet and confer" required by *Cal Rules Ct, Rule 3.724(8)* if discovery of ESI information is reasonably likely to be sought. It is *imperative* that a technical expert be retained before the actual meet and confer. A brief consultation early on can provide valuable input related to e-discovery strategies and cost saving methodologies and may help reduce, if not eliminate, the misconceptions and miscommunications common to the e-discovery process.

- The CCP and Cal Rules of Court amendments were modeled in large part on the 2006 Federal Rules of Civil Procedure amendments governing e-discovery in federal courts. Because there is a strong public policy in favor of interpreting similar statutes dealing with the same subject matter in a similar fashion, a

federal court's interpretation of federal statutes will guide the interpretation of California statutes modeled after those federal provisions [*Scripps Memorial Hosp., Inc. v. California Employment Comm'n* (1944) 24 C2d 669, 677, 151 P2d 109 ("it is presumed that the California Legislature had those interpretations in mind"); *Kahn v. Kahn* (1977) 68 CA3d 372, 387, 137 CR 332] . Therefore, attorneys may wish to consult federal cases interpreting e-discovery statutes, in the absence of California case law.

**Cross References:**

Ch. 2, Governing Law in Electronic Discovery, 2.03-2.13.

Sanctions for breach of attorney's discovery obligations, see Ch. 13, Seeking or Opposing Sanctions for Noncompliance.

Interpretation of California e-discovery rules, see DeMeo, *California Deposition and Discovery Practice, Ch. 2A, Discovery of Computer Records, § 2A.02-§ 2A.03* (Matthew Bender).

Electronic evidence in federal practice, see Moore's Federal Practice, Ch. 37A, Discovery of Computer-Based Information (Matthew Bender 3d ed.).

Discovery of computer records in federal cases, see Matthew Bender(R) Practice Guide: Federal Pretrial Civil Procedure in California, Ch. 23, Methods of Discovery.



108 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

II. UNDERSTANDING E-ELECTRONIC DISCOVERY DUTIES OWED TO CLIENTS

1-3 MB Practice Guide: CA E-Discovery and Evidence 3.03

AUTHOR: Diane E. Barry, Esq.

3.03 CHECKLIST: Understanding Electronic Discovery Duties Owed to Clients.

☐ Explain discovery to clients.

Authority:

CCP § 2031.230; Maldonado v. Superior Court (2002) 94 CA4th 1390, 1396, 115 CR2d 137

Discussion:

See 3.04, 3.05[1]

☐ Acquire reasonable understanding of client's ESI and computer systems, or associate expert who has this knowledge.

Authority:

Cal Rules Ct, Rule 3.724(8)

Discussion:

See 3.05 [3], 3.06

☐ With participation of client, draft and send litigation hold notice to client's "key players" and IT personnel.

Authority:

Zubulake v. UBS Warburg LLC (SDNY 2004) 220 FRD 212, 218

Discussion:

See 3.05[4]

- ☐ Remain actively involved in e-discovery or monitor e-discovery collection.

Authority:

Zubulake v. UBS Warburg LLC (SDNY 2004) 229 FRD 422, 435

Discussion:

See 3.05[2], 3.06

- ☐ With participation of client, client's "key players" and IT personnel, create document describing client's e-documents that are available for discovery, their current format and format desired for discovery, and timeline for production of each format.

Authority:

Cal Rules Ct, Rule 3.724; Zubulake v. UBS Warburg LLC (SDNY 2004) 220 FRD 212, 218 ; Nat'l Ass'n of Radiation Survivors v. Turnage (ND Cal 1987) 115 FRD 543, 552

Discussion:

See 3.05[2]-[4], 3.06[1]



109 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

II. UNDERSTANDING E-ELECTRONIC DISCOVERY DUTIES OWED TO CLIENTS

1-3 MB Practice Guide: CA E-Discovery and Evidence 3.04

AUTHOR: Diane E. Barry, Esq.

3.04 Clients Bear Ultimate Responsibility to Preserve and Produce All Relevant Electronically Stored Records.

Ultimately, the duty to preserve evidence resides with the party to the litigation. Every party has a general duty to preserve relevant evidence if litigation is reasonably anticipated. This duty ensures that potentially relevant evidence is not lost or destroyed [*CCP* § 2023.010; *Cedars-Sinai Med. Ctr. v. Sup. Ct.* (1998) 18 C4th 1, 12, 74 CR2d 248, 954 P2d 511 ; *Dodge, Warren, & Peters Ins. Services, Inc. v. Riley* (2003) 105 CA4th 1414, 1418-1420, 130 CR2d 385 ; see *Zubulake v. UBS Warburg LLC* (SDNY 2004) 229 FRD 422, 436 ("[a]t the end of the day, however, the duty to preserve and produce documents rests on the party")].

Example:

Defendant foreign corporation was sued for alleged RICO violations in connection with financing scheme. Defendant failed to respond to basic discovery requests or to file an opposition to the ensuing motion to compel. When defense counsel appeared in court to answer an order to show cause and to discuss discovery, he was unable to answer the court's questions about what the client was doing to locate ESI or when promised materials might arrive from abroad. The court imposed monetary sanctions against the client [*Bank of Mongolia v. M&P Global Financial Servs.* (SD Fla 2009) 2009 US Dist LEXIS 39239, at *15-*24] .

Cross References:

Preservation of evidence, see *Ch. 5, Initial Procedures in Electronic Discovery--Notice, Document Preparation, Meeting and Conferencing, and Case Management Conference*, 5.03-5.08.

Preservation of ESI evidence in the discovery context, see *Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 5, Discovery of Electronic Information*, 5.06.

Sample form for preservation order, see *Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 5, Discovery of Electronic Information*, 5.47.

Preservation of evidence in the context of discovery generally, see *Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 14, Preservation of Evidence*, 14.17.



110 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

II. UNDERSTANDING E-ELECTRONIC DISCOVERY DUTIES OWED TO CLIENTS

1-3 MB Practice Guide: CA E-Discovery and Evidence 3.05

AUTHOR: Diane E. Barry, Esq.

3.05 Attorneys' Duties to Clients Regarding Electronic Discovery Obligations.

3.05[1] Attorneys Have Duty to Explain Discovery to Clients. Attorneys have an affirmative duty to explain discovery obligations to their clients. This discussion should include the types of records that are discoverable and relevant and the need to use appropriate collection and preservation methods [*CCP § 2031.230* (statement of inability to comply with inspection demand certifies that diligent search and reasonable inquiry has been made); *Maldonado v. Superior Court* (2002) 94 CA4th 1390, 1396, 115 CR2d 137 ("diligent search and a reasonable inquiry" is required to comply with demand for documents)].

Examples:

- Defendant performed its own document collection with little input or follow-up from its counsel. The non-legal staff person responsible for collection did not realize until well into the process that e-files were "documents" that he should have been collecting. The resulting document production was both incomplete and late. Due to failure to preserve, many paper and e-documents were lost. The court found that defense counsel violated *Federal Rules of Civil Procedure Rule 26* by failing to explain to its client what types of information would be relevant and responsive to document requests and to ask how and where relevant documents were maintained. The court noted that attorneys have an affirmative duty to make a reasonable effort to instruct their clients about discovery obligations, and to make reasonable inquiries about collection process and progress [*Metropolitan Opera Ass'n v. Local 100, Hotel Employees & Restaurant Employees Int'l Union* (SDNY 2003) 212 FRD 178, 222].
- Defendants involved in a lawsuit over a failed art purchase transaction did not produce a spreadsheet of their art holdings until after being ordered to do so in response to a motion to compel discovery. After defendants produced the spreadsheet, plaintiff demanded any drafts of the spreadsheet, and defendant produced what purported to be three electronic versions. Plaintiff moved for an order authorizing a forensic examination of defendant's computer. Defendants then revealed that during the litigation they had hired the son of a friend to reinstall the computer's operating system, and had backed up the data onto compact disks. Plaintiff withdrew the motion, contending the forensic examination would be

useless, and asked the court for sanctions consisting of (1) additional time to depose the defendant about the spreadsheet and other electronically-stored documents, at her expense; (2) an order directing the defendants to identify the person who created the spreadsheet; (3) payment of costs incurred by the plaintiff in bringing this motion, including attorneys' fees; and (4) an adverse inference that the defendants had understood that they had in fact purchased the work of art and added it to their personal collection. The court held that the preservation obligation runs first to counsel, who has a duty to advise his client of the type of information potentially relevant to the lawsuit and of the necessity of preventing its destruction. The court granted all of plaintiff's requests except for the adverse inference sanction [*Green v. McClendon* (SDNY 2009) 262 FRD 284] .

- Defendant correctional facility gathered requested medical documents, but failed to include related cover sheets containing information relevant to the plaintiff's claims. The defense argued that neither defendant nor counsel had known about the existence of the sheets until they were mentioned in the depositions of two former employees. The court found that counsel had a duty to inform itself about the evidence in its client's possession, and to adequately counsel the client regarding the kinds of records that were responsive. Therefore, ignorance was not an acceptable explanation [*Tarlton v. Cumberland County Correctional Facility* (DNJ 2000) 192 FRD 165, 170] .

Cross References:

Planning e-discovery, see *Ch. 4, Planning Electronic Discovery*, 4.01-4.10.

Duty to communicate with clients, see *California Forms of Pleading and Practice*, Ch. 72, *Attorney Practice and Ethic*, 72.271 (Matthew Bender).

3.05[2] Attorneys Have Duty to Be Actively Involved in or Monitor E-Discovery Collections. Attorneys have a duty to be actively involved in a client's evidence collection process, or, at a minimum, to monitor compliance with discovery requirements [see *CCP § 2031.230* (statement of inability to comply with inspection demand certifies that diligent search and reasonable inquiry has been made); *Maldonado v. Superior Court* (2002) 94 CA4th 1390, 1396, 115 CR2d 137 ("diligent search and a reasonable inquiry" is required to comply with demand for documents); *Thomas v. Lusk* (1994) 27 CA4th 1709, 1718, 34 CR2d 265 (discussion of duty to conduct reasonable search so as to inform choices regarding litigation conduct)].

Examples:

- Defendant did not begin ESI preservation and collection process until at least a year after the complaint was filed. The litigation hold notice sent to employees did not specifically mention ESI. E-mails were deleted and could not be restored. Imposing discovery sanctions, the court noted that the ill effects of the client's conduct could well have been mitigated had counsel been more diligent in assisting the client [*Zubulake v. UBS Warburg LLC* (SDNY 2004) 229 FRD 422, 435] .

- Defendant union local performed its own document collection with little input or follow up from its counsel. The non-legal staff person responsible for collection did not realize until well into the process that e-files were "documents" that he should have been collecting. He missed many custodians entirely. The resulting document production was both incomplete and late. Due to failure to preserve, many paper and e-documents were lost. Imposing sanctions, the court observed that attorneys have an affirmative duty to make reasonable inquiries regarding collection process and progress [*Metropolitan Opera Ass'n v. Local 100, Hotel Employees & Restaurant Employees Int'l Union* (SDNY 2003) 212 FRD 178, 222] .

Cross References:

Duty to Preserve Electronic Evidence, see *Matthew Bender(R) Practice Guide: California Civil Discovery*, Ch. 5, *Discovery of Electronic Information*, 5.07.

Duty to preserve electronic evidence, see *California Forms of Pleading and Practice*, Ch. 190, *Discovery: Scope, Regulation, and Timing*, 190.24[5] (Matthew Bender).

3.05[3] Attorneys Must Have Reasonable Understanding of Client's Electronically Stored Information and Computer Systems. Counsel have an affirmative duty to be informed about a client's ESI and computer systems, in order to assist the client in responding to both formal discovery and informal requests for information from opposing counsel and the court [see *CCP § 2031.230* (statement of inability to comply with inspection demand certifies that diligent search and reasonable inquiry has been made); *Cal Rules Ct, Rule 3.724(8)* (list of topics regarding client's systems that must be discussed with opposing counsel prior to case management conference); *Maldonado v. Superior Court (2002) 94 CA4th 1390, 1396, 115 CR2d 137* ("diligent search and a reasonable inquiry" is required to comply with demand for documents)].

Examples:

- Defendant correctional facility gathered requested medical documents, but failed to include related cover sheets containing information relevant to the plaintiff's claims. Defendants argued that neither the client nor counsel had known about the existence of the sheets until they were mentioned in the depositions of two former employees. The court found that counsel had a duty to be informed about the evidence in their client's possession. Ignorance was not an acceptable explanation [Tarlton v. Cumberland County Correctional Facility, (DNJ 2000) 192 FRD 165, 170].

- Defendant represented to both opposing counsel and to the court that it did not have information in a computer format for the time period requested. A year later, at the deposition of the vice president, the deponent informed the parties that defendant did have the requested information at one time, but only for a two-year time period. By the time of the deposition, the data for the relevant time period had been overwritten. The court noted that whether or not defense counsel had intentionally misled opposing counsel, defense counsel's inquiries about the computer systems had been "deficient" [*GTfM, Inc. v. Wal-Mart Stores, Inc. (SDNY 2000) 2000 US Dist LEXIS 3804, at *5-*6*].



Cross References:

Gathering and Producing ESI, see Ch. 9, *Gathering and Producing Electronically Stored Information*.

Obtaining evidence about how ESI is maintained, see *Matthew Bender(R) Practice Guide: California Civil Discovery*, 5.08.

3.05[4] Attorneys Have Duty to Assist and Monitor Litigation Holds. A litigation hold is a process whereby corporate clients identify materials relevant to discovery in an ongoing or imminent litigation matter. An attorney has a duty to be involved in, or at a minimum, remain informed about, a client's discovery response process. This duty includes working with clients to establish a litigation hold and following up with persons to whom a litigation hold notice is sent [*Cedars-Sinai Med. Ctr. v. Superior Court (1998) 18 C4th 1, 12-13, 74 CR 2d 248, 954 P2d 511* ("[m]odern 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 ..."); *Maldonado v. Superior Court (2002) 94 CA4th 1390, 1396, 115 CR2d 137* ("diligent search and a reasonable inquiry" is required to comply with demand for documents); *Zubulake v. UBS Warburg LLC (SDNY 2004) 229 FRD 422, 432-434* (counsel's duty to work with client to preserve and produce all relevant non-privileged information); *Zubulake v. UBS Warburg LLC (SDNY 2003) 220 FRD 212, 218-219* (describing

litigation hold process)].

Example:

Defendant's litigation hold was both poorly planned and poorly implemented. The hold notices were sent out, but not to all of the custodians who should have received them. Those who did receive notice often did not understand that the litigation hold applied to them. Those who did understand that the hold applied to them often did not understand the broad sweep of materials that needed to be preserved. There was also little or no follow-up with any of the custodians who had received the notice. As a result, defendant was unable to produce all relevant and responsive documents in its possession or control, and its pension administration purged and destroyed relevant paper documents and e-records as part of the regular records retention schedule. The court sanctioned counsel for failure to work with their client to establish "a coherent and effective system to faithfully and effectively respond to discovery requests" [*Nat'l Ass'n of Radiation Survivors v. Turnage* (ND Cal 1987) 115 FRD 543, 556] .



Cross References:

Gathering and Producing ESI, see Ch. 9, Gathering and Producing Electronically Stored Information.

Obtaining evidence about how ESI is maintained, see *Matthew Bender(R) Practice Guide: California Civil Discovery*, 5.08.

Responding parties duties, see *Matthew Bender(R) Practice Guide: California Civil Discovery*, 5.12.



111 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

II. UNDERSTANDING E-ELECTRONIC DISCOVERY DUTIES OWED TO CLIENTS

1-3 MB Practice Guide: CA E-Discovery and Evidence 3.06

AUTHOR: Diane E. Barry, Esq.

3.06 Attorneys' Responsibilities for Client Electronic Discovery Responses.

3.06[1] Attorneys Have Duty to Conduct Reasonable Investigation of Foundation for Electronic Discovery Responses and Representations. An attorney signing an e-discovery request is making a personal certification that the request is not made for the purpose of harassment or other discovery abuse [see *CCP § 2023.010(a)*]. Similarly, an attorney signing an e-discovery response certifies that he or she personally has made reasonable inquiry to support the response [see *Maldonado v. Superior Court (2002) 94 CA4th 1390, 1396, 115 CR2d 137* ("diligent search and a reasonable inquiry" is required to comply with demand for documents)]. If counsel does not make a reasonable inquiry before responding, counsel can be held responsible for response inadequacies [*CCP § 2031.030* (counsel must represent that diligent search and reasonable inquiry have been made when party is unable to comply with inspection demand); *CCP § 2023.010(d)-(f)* (discovery abuses include non-responses and evasive responses); *Maldonado v. Superior Court (2002) 94 Cal. App. 4th 1390, 1396, 115 Cal. Rptr. 2d 137*].

Examples:

- Despite court rulings that discovery requests were not overbroad or burdensome, client continued to pick and choose what it would respond to. At least three partners at the outside law firm knew that client was not responding responsibly to discovery. Counsel's conduct at depositions and before the court assisted in client's discovery misconduct. The law firm was sanctioned for its part in aiding client discovery abuse [*1100 West, LLC v. Red Spot Paint & Varnish Co. (SD Ind 2009) 2009 US Dist LEXIS 47439, at *93-*95*].
- Defendant performed its own document collection with little input or follow-up from its counsel. The resulting document production was both incomplete and late, and many documents were lost due to failure to preserve. Both the court and opposing counsel made repeated inquiries regarding the adequacy of the document production. Defense counsel represented multiple times, orally and in writing, that the production was full and complete. The court noted that counsel have an affirmative duty to make a reasonable inquiry into the basis of the client's discovery responses and to "stop and think about the legitimacy of the responses." The court concluded that defense counsel ought to have known that the

responses had been improperly prepared and should not have made its representations regarding the production without further investigation. Monetary sanctions were granted against the defendant and its counsel [*Metropolitan Opera Ass'n v. Local 100, Hotel Employees & Restaurant Employees Int'l Union* (SDNY 2003) 212 FRD 178, 222] .

► **Cross Reference:**

Sanctions for e-discovery abuses, see *California Forms of Pleading and Practice*, Ch. 190, *Discovery: Scope, Regulation, and Timing*, 190.24[6] (Matthew Bender).

3.06[2] Late or Incomplete Electronic Discovery Responses Are Sanctionable. Failure to respond or to submit to an authorized method of discovery is subject to sanction [CCP § 2023.010(d)]. If a response is so late or so incomplete as to be deemed no answer at all, the conduct can be sanctionable [CCP 2023.010(d); see *Karlsson v. Ford Motor Company* (2006) 140 CA4th 1202, 1215-1216, 45 CR3d 265 (eve of trial document production was tantamount to non-production, as party was deprived of ability to prepare for trial, and supported award of evidentiary sanctions)].

► **Cross References:**

See 3.06[3][c].

Sanctions for e-discovery abuses, see Ch. 13, *Seeking or Opposing Sanctions for Noncompliance*; see also *California Forms of Pleading and Practice*, Ch. 190, *Discovery: Scope, Regulation, and Timing*, 190.24[6] (Matthew Bender).

Types of sanctions available for discovery misuse, see *Matthew Bender(R) Practice Guide: California Civil Discovery*, Ch. 3, *Sanctions*, 3.10.

3.06[3] Responsibility for Client Electronic Discovery Misconduct.

3.06[3][a] Attorney Is Not Responsible for Client Misconduct Not Known to Attorney. Sanctions will not be imposed if the attorney did not know, and could not reasonably have known, of client misconduct regarding discovery responses [*Biles v. Exxon Mobil Corp.* (2004) 124 CA4th 1315, 1325, 22 CR3d 282] .

3.06[3][b] Attorney Bears Responsibility for Client Misconduct Known or Assisted by Counsel. The attorney may be sanctioned for client misconduct if the evidence shows that the attorney is to blame in connection with the client's failure to comply with discovery [*Weinkauff v. Superior Court* (1966) 64 C2d 662, 665, 51 CR 100, 414 P2d 36 (approving trial court award of sanctions against attorney for his client's failure to answer interrogatories, when failure was attributable primarily to counsel)].

3.06[3][c] Bases for Supporting Award of Sanctions Against Attorney. There are multiple bases for supporting an award of sanctions, discipline by the California State Bar, or criminal penalties when an attorney knowingly or recklessly assists a client in discovery abuse or otherwise adopts, assists, or abets a client in misleading the court or other judicial officers. For example:

- An attorney is duty bound not to mislead judges, juries, or any other judicial officer [B&P Code § 6068(d); *Cal Rules Prof Conduct*, Rule 5-200(B) (lawyer may not seek to mislead court by false statement of fact or law); *Cal Rules Prof Conduct*, Rule 5-220 (lawyer must not suppress evidence that lawyer or the lawyer's client has legal obligation to reveal or to produce)].
- An attorney may be subject to discipline by the California State Bar, including suspension and disbarment, for participating in the destruction or suppression of evidence [B&P Code § 6106 (act of moral turpitude, dishonesty or corruption is cause for disbarment or suspension)].

- An attorney who destroys or suppresses evidence may be prosecuted criminally [*Pen Code* § 135 (destruction of evidence is misdemeanor); see *Pen Code* §§ 7(1), (5) ("willfully" and "knowingly" defined)].
- An attorney who signs a false certification or affidavit may be sanctioned for discovery abuse [see *CCP* § 2023.010(e), (f)].
- An attorney who signs a false certification or affidavit may be prosecuted for perjury [*Pen Code* § 118a (false affidavit is perjury)].

Examples:

- Despite court rulings that discovery requests were not overbroad or burdensome, client continued to pick and choose what it would respond to. At least three partners at the outside law firm knew that client was not responding responsibly to discovery. Counsel's conduct at depositions and before the court assisted in client's discovery misconduct. Accordingly, the law firm was sanctioned for its part in aiding client discovery abuse [*1100 West, LLC v. Red Spot Paint & Varnish Co. (SD Ind. 2009) 2009 US Dist. LEXIS 47439, at *93-*95*].
- In a patent infringement action, plaintiff failed to produce more than 46,000 relevant e-mails and e-documents that had been requested in discovery, and which plaintiff had agreed to produce. Although plaintiff's counsel became aware of the failure during final trial preparation, it chose not to bring the matter to the attention of the court or opposing counsel. When the discrepancies were discovered at trial, counsel told the court that the e-mails had been discovered, but had not been produced because they were not responsive to any prior discovery request. The court found that the plaintiff's outside attorneys had either intentionally or recklessly assisted their client in committing a tremendous discovery violation through poor e-discovery practices. The court issued monetary sanctions against the client and against the attorneys--in-house counsel and outside counsel. The court also referred the attorneys to the California State Bar for potential discipline for violations of *Cal Rules Prof Conduct, Rules 5-200 and 5-220* [*Qualcomm Inc. v. Broadcom Corp. (SD Cal 2008) 2008 US Dist LEXIS 911, at *64, vacated in part, Qualcomm Inc. v. Broadcom Corp. (SD Cal 2008) 2008 US Dist LEXIS 16897*].



Cross References:

Types of sanctions available for discovery misuse, see *Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 3, Sanctions, 3.10*.

Motion seeking and opposing sanctions, see *Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 3, Sanctions, 3.11, 3.13-3.14*.

Sanctions for e-discovery abuses, see *California Forms of Pleading and Practice, Ch. 190, Discovery: Scope, Regulation, and Timing, 190.24[6]* (Matthew Bender).

Attorney responsibilities and sanctions for e-discovery abuses, see DeMeo, *California Deposition and Discovery Practice, Ch. 2A, Discovery of Computer Records, § 2A.05, § 2A.08* (Matthew Bender).



112 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

III. UNDERSTANDING ELECTRONIC DISCOVERY DUTIES OWED TO COURTS AND OPPOSING COUNSEL

1-3 MB Practice Guide: CA E-Discovery and Evidence 3.07

AUTHOR: Diane E. Barry, Esq.

3.07 CHECKLIST: Understanding Electronic Discovery Duties Owed to Courts and Opposing Counsel.

- ☐ Prepare for meet and confer required by *Cal Rules Ct, Rule 3.724(8)* by sending ESI Discovery Notice Letter to opposing counsel.

Authority:

Cal Rules Ct, Rule 3.724(8)

Discussion:

See 3.08[3]

Form:

See *Ch 5, Initial Procedures in Electronic Discovery--Notice, Document Preservation, Meeting and Confering, and Case Management Conference, 5.29.*

- ☐ Prepare for meet and confer required by *Cal Rules Ct, Rule 3.724(8)* by working with client to determine extent of ESI, desirable or required formats, and timing required for production.

Authority:

Cal Rules Ct, Rule 3.724(8); Zubulake v. UBS Warburg LLC (SDNY 2004) 220 FRD 212, 218 ; Nat'l Ass'n of Radiation Survivors v. Turnage (ND Cal 1987) 115 FRD 543, 552

Discussion:

See 3.08[2], 3.09

- ☐ Meet and confer with opposing counsel.

Authority:

Cal Rules Ct, Rule 3.724(8); Cal Rules Ct, Rule 3.728(13)

Discussion:

See 3.08[1]

- ☐ Ensure reasonable, good faith basis for e-discovery representations made to court and opposing counsel.

Discussion:

See 3.09

- ☐ Refrain from discovery-related obstructionist tactics.

Discussion:

See 3.10



113 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

III. UNDERSTANDING ELECTRONIC DISCOVERY DUTIES OWED TO COURTS AND OPPOSING COUNSEL

*1-3 MB Practice Guide: CA E-Discovery and Evidence 3.08***AUTHOR:** Diane E. Barry, Esq.**3.08 Attorneys Must Meet and Confer in Good Faith on Electronic Discovery Issues.**

3.08[1] Attorneys Must Arrange to Meet and Confer. The attorneys are required to meet and confer on e-discovery issues [see *Cal Rules Ct, Rule 3.724(8)* (list of ESI-related topics on which counsel must meet and confer prior to initial case management conference); *CCP § 2023.010(i)* (failure to meet and confer in good faith is sanctionable discovery abuse); *Liberty Mutual Fire Ins. Co. v. LcL Administrators (2008) 163 CA4th 1093, 1104, 78 CR3d 200* (fact that counsel repeatedly ignored meet and confer letters formed separate grounds for discovery sanctions under *CCP § 2023.010(i)* for failure to meet and confer in good faith); see also *Rico v Mitsubishi Motors Corp. (2007) 42 C4th 807, 818, 68 CR3d 758, 766* ("[a]n attorney has an obligation not only to protect his client's interests but also to respect the legitimate interests of fellow members of the bar, the judiciary, and the administration of justice")].

**Timing:**

The parties must meet and confer no later than 30 calendar days before the initial case management conference, unless the court orders another time period [*Cal Rules Ct, Rule 3.724(8)*]. In practice, this means that the meeting ordinarily will take place in the first 30 to 60 days of the matter.

**Cross Reference:**

Detailed discussion of meet and confer requirement, see *Ch. 5, Initial Procedures in Electronic Discovery--Notice, Document Preparation, Meeting and Conferencing, and Case Management Conference, 5.14-5.25.*

3.08[2] Good Faith Conduct Requires Preparation. In order to meet and confer on e-discovery issues in good faith, attorneys must be prepared to resolve any discovery disputes and set a discovery schedule [*Cal Rules Ct, Rule 3.724*]. In the e-discovery context, this means understanding the client's ESI, production formats, production timing, collection and preservation issues, cost shifting (if any), and procedures for reclaiming items inadvertently produced. To come to the meet and confer unprepared to address the required issues is to meet and confer in bad faith [*Cal Rules Ct, Rule 3.724(8)* (list of ESI-related topics on which counsel must meet and confer before initial case management conference); *CCP § 2023.010(i)* (failure to meet and confer in good faith is a sanctionable discovery abuse); *Liberty Mutual Fire Ins. Co. v. LcL Administrators (2008) 163 CA4th 1093, 1104, 78 CR3d 200* (fact that counsel repeatedly

ignored meet and confer letters formed separate grounds for discovery sanctions under *CCP* § 2023.010(i) for failure to meet and confer in good faith)].



Strategic Points:

- Most of the problems related to good faith preparation are grounded in counsel's limited understanding of the client's computer systems and available ESI. Unless counsel is properly informed, he or she cannot communicate effectively with opposing counsel and the court in discovery papers and hearings.
- Difficulties can arise when clients want to conduct their own document collection and do not want to pay outside counsel fees for this process. In these circumstances, the attorney should monitor the client's process and progress, and know what the client has and does not have, and why. The attorney must be able to accurately advise the court and opposing counsel regarding status and issues
- If difficulties arise in understanding a client's technology or the steps and timing required to produce particular types of e-discovery, counsel should obtain technical help. Even a few hours of technical consultation can provide substantial assistance in understanding the process and timing for each media type involved in the matter. Timing is also critical. *Cal Rules Ct, Rule 3.724(8)* requires discussing ESI issues with opposing counsel at least 30 days before the initial case management conference. Counsel should obtain technical assistance well in advance of the meet and confer date.
- Counsel must have a reasonable basis for representations made, and those representations must be reasonably accurate. As a practical matter, counsel should speak the truth as he or she knows it, after reasonable inquiry. If counsel doesn't know the answer to a question, he or she should offer to research the issue and get back to opposing counsel or to the court with an answer. The alternative is to be found to have made a substantive misrepresentation to opposing counsel or worse, to the court.



Cross References:

Detailed discussion of meet and confer requirement, see *Ch. 5, Initial Procedures in Electronic Discovery--Notice, Document Preparation, Meeting and Conferencing, and Case Management Conference, 5.14-5.25.*

Gathering and Producing ESI, see *Ch. 9, Gathering and Producing Electronically Stored Information.*

Obtaining evidence about how ESI is maintained, see *Matthew Bender(R) Practice Guide: California Civil Discovery, 5.08.*

3.08[3] Good Faith Conduct Requires Notice to Opposing Counsel That Discovery of Electronically Stored Information Will Likely Be Sought. If discovery of ESI information is reasonably likely to be sought in the proceeding, counsel should notify opposing counsel (or a pro se party) in writing. This allows the parties and their attorneys to prepare to meet and confer on issues related to e-discovery before the initial case management conference [see *Cal Rules Ct, Rule 3.724(8)* (listing e-discovery topics on which counsel must meet and confer)].



Timing:

The notice letter should be sent as soon as possible and well in advance of meet and confer date, which is at least 30 days before the date set for the initial case management conference [see *Cal Rules Ct. Rule*

3.724(8)].

 Cross Reference:

Detailed discussions of Rule 3.724(8) Notice, see *Ch. 4, Planning E-Discovery*, 4.18; see also *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference*, 5.09-5.13.

Examples:

■ In a products liability case regarding a seatbelt design in a minivan, defendant's counsel consistently misinformed plaintiff's counsel, the discovery referee, and the court, about what documents, witnesses, and information were available and failed to produce materials defendant had agreed to produce, or materials ordered produced by the court. The discovery referee found that, among other discovery violations, defendants' conduct was not in good faith [*Karlsson v. Ford Motor Co. (2006) 140 CA4th 1202, 1211, 45 CR3d 265, 272*] .

■ In a breach of contract action, defendant, faced with ordinary discovery requests, made "vacuous, meaningless responses," propounded no discovery of its own, and ignored meet and confer letters from opposing counsel. The court noted that defendant's conduct "reeked of bad faith" and that its failure to respond to meet and confer requests provided a sufficient independent ground to support discovery sanctions under CCP § 2023.010(i) [*Liberty Mutual Fire Ins. Co. v. LcL Administrators (2008) 163 CA4th 1093, 1104, 78 CR3d 200, 208*] .

 Cross References:

Detailed discussion of meet and confer requirement, see *Ch. 5, Initial Procedures in Electronic Discovery--Notice, Document Preparation, Meeting and Conferencing, and Case Management Conference*, 5.14-5.25.

Notice Regarding Intent to Conduct ESI discovery, see *Ch. 5, Initial Procedures in Electronic Discovery--Notice, Document Preparation, Meeting and Conferencing, and Case Management Conference*, 5.09-5.13.



114 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

III. UNDERSTANDING ELECTRONIC DISCOVERY DUTIES OWED TO COURTS AND OPPOSING COUNSEL

1-3 MB Practice Guide: CA E-Discovery and Evidence 3.09

AUTHOR: Diane E. Barry, Esq.

3.09 Attorneys Must Have Good Faith Basis for Electronic Discovery Representations Made to Court and Opposing Counsel.

3.09[1] Discovery Response Certifications and Court Filings. An attorney who signs a discovery response or other certification affirms that the contents are true and correct under penalty of perjury [*see CCP § 2015.5*]. An attorney's signature also certifies that a reasonable inquiry has been made, and that the discovery or response is not offered for any improper or abusive purpose. It is both an ethical and a criminal violation to knowingly or willfully sign an untruthful certification [*Pen Code §§ 118a* (false affidavit is perjury), *125* (unqualified statement which is not known to be true is the same as knowingly making a false statement); *B&P Code § 6068(d)* (duty as an attorney to employ only those means as are consistent with the truth); *CCP § 2023.010(e), (f)* (discovery abuse); *Cal Rules Prof Conduct, Rule 5-200(B)* (lawyer may not seek to mislead court by false statement of fact or law); *Cal Rules Prof Conduct, Rule 5-220* (lawyer must not suppress evidence that the lawyer or the lawyer's client has legal obligation to reveal or to produce)].

Example:

In a bankruptcy matter in which the issues pertained to the motives behind certain transfers, the defendants made multiple misrepresentations to the court that resulted in sanctions. The court found that the misrepresentations stemmed either from negligent document production or willful discovery malfeasance. First, defense counsel represented to the court that its clients had produced all documents regarding transfers, and that the search for documents had been diligent. Two supplemental productions later--many from counsel's own files--and the court had had enough. The court imposed monetary sanctions on the grounds that clearly all documents had not been produced when counsel made their representations to the court, and that just as clearly, the search for documents had been by no means "diligent." The court also found counsel's account of why particular documents had not been discovered in a timely fashion "ridiculous." Counsel fared no better in their e-production. When discussing discovery of e-mail from backup tapes during court hearings, defense counsel repeatedly minimized the possible value of tapes and e-mails to the court. After sampling turned up thousands of "hot" documents, the court concluded that counsel's statements in this area had been either reckless or deliberately misleading [*Kipperman v. Onex Corp. (ND GA 2009) 2009 US Dist LEXIS 44457, at *59-*61*].



Cross Reference:

Duty of competence, see *California Forms of Pleading and Practice*, Ch. 72, *Attorney Practice and Ethic*, 72.270 (Matthew Bender).

3.09[2] Oral Communications and Correspondence. Attorneys have a duty to communicate truthfully with opposing counsel and the court, even when those communications are not made in formal discovery hearings. A member of the California State Bar may not seek to mislead the judge, judicial officer, or jury by an artifice or false statement of fact or law [*Cal Rules Prof Conduct*, Rule 5-200(B); *Williams v. Superior Court* (1996) 46 CA4th 320, 330-331, 53 CR2d 832 ("[h]onesty in dealing with the courts is of paramount importance, and misleading a judge is, regardless of motives, a serious offense")].

Example:

In a letter to plaintiff's counsel, defense attorney included documents forwarded to him by defendant that were responsive to a prior discovery request. Without further inquiry, the attorney represented that the additional documents had been discovered after a "significant search." The court held that this was a certification made without reasonable inquiry that could support imposition of sanctions against the attorney [*Phinney v. Paulshock*, (DNH 1998) 181 FRD 185, 203-204] .

 Cross Reference:

Detailed discussion of meet and confer requirement, see Ch. 5, *Initial Procedures in Electronic Discovery--Notice, Document Preparation, Meeting and Conferring, and Case Management Conference*, 5.14-5.25.

3.09[3] Communications Via Social Networking Sites. The widespread use of social networking sites such as Facebook and MySpace has increased the value of these sites as a potential source of information that may be useful in litigation. People post large amounts of information about themselves and their lives on the sites, and can control the level of information viewable by members of the public through privacy settings, and by granting access to their postings by designating people as their friends (known as "friending" people). This is an emerging area with developing law.

The information people post on social networking sites has the potential to be useful in litigation, but collecting that information is subject to ethical constraints against deception and contact with represented parties. For example, the Philadelphia Bar Association has issued an ethical opinion concluding that having a paralegal make a "friend" request to an unrepresented witness for the purposes of gathering information that could be useful in impeaching the witness violates ethical rules proscribing deceitfulness in dealing with members of the public in connection with a lawyer's representation of a client [Philadelphia Bar Association Professional Guidance Committee Opinion 2009-02 at p. 3 (March 2009)]. Moreover, if the witness (or an opposing party) is represented by counsel, "friending" them is the type of purposeful contact that would likely constitute personal contact with a represented party.

 Cross References:

Social networking sits as a source of ESI, see 1.32[6].

Discussion of social networking sites and the Federal Stored Communications Act, see 6.17[6].



115 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

III. UNDERSTANDING ELECTRONIC DISCOVERY DUTIES OWED TO COURTS AND OPPOSING COUNSEL

1-3 MB Practice Guide: CA E-Discovery and Evidence 3.10

AUTHOR: Diane E. Barry, Esq.**3.10 Attorneys Must Refrain From Discovery-Related Obstructionist Tactics.**

3.10[1] Running Up Electronic Discovery Costs Is Improper. Issuing e-discovery requests for the purpose of running up costs is a sanctionable discovery abuse [CCP § 2023.010(c); Judicial Council of California Invitation to Comment, Discussion, p. 2 ("[t]he large volume of electronically stored information sometimes can significantly increase the amount of time and cost of searching for information")].

➤ **Cross Reference:**

Misuse of discovery process, see DeMeo, *California Deposition and Discovery Practice*, Ch. 42, *Discovery Sanctions*, 42.02 (Matthew Bender).

3.10[2] Demanding Unnecessary Electronic Discovery Is Improper. Discovery may not be used in a manner or to an extent that causes unwarranted annoyance, embarrassment, or oppression, or undue burden and expense [CCP § 2023.010(c)].

➤ **Cross Reference:**

Misuse of discovery process, see DeMeo, *California Deposition and Discovery Practice*, Ch. 42, *Discovery Sanctions*, 42.02 (Matthew Bender).

3.10[3] Negligence or Lack of Basic Knowledge Regarding Electronic Discovery Requirements Constitutes Incompetence. When an attorney undertakes a representation, he or she must act competently. A "competent" attorney must be able to apply the diligence, learning and skills reasonably necessary for the engagement [*Cal Rules Prof Conduct*, Rule 3-110 (failure to act competently; competence by learning or association)].

In matters that require e-discovery skills, an attorney must personally possess the skills required, be able to learn those skills adequately in time to use them at appropriate points in the course of the representation, or must associate with or engage someone who has the requisite skills. An attorney need not act willfully to destroy or fail to preserve ESI to be sanctioned. Simple negligence will suffice [*Zubulake v. UBS Warburg LLC* (SDNY 2004) 220 FRD. 212, 220 ("Once the duty to preserve attaches, any destruction of documents is, at a minimum, negligent"); *Kohan v. Cohan* (1991) 229

CA3d 967, 971, 280 CR 474 (willfulness is not required to impose sanctions, interpreting former CCP § 2023(b)(1) (now CCP § 2023.030(a)); see *Ten Eyck v. Indus. Forklifts Co.* (1989) 216 CA 3d 540, 545-546, 265 CR 29 (counsel was duty-bound to know rules of civil procedure)].

**Cross Reference:**

Duty of competence, see *California Forms of Pleading and Practice*, Ch. 72, *Attorney Practice and Ethic*, 72.270 (Matthew Bender).



116 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

IV. UNDERSTANDING ELECTRONIC DISCOVERY PRIVILEGE WAIVER ISSUES

1-3 MB Practice Guide: CA E-Discovery and Evidence 3.11

AUTHOR: Diane E. Barry, Esq.

3.11 CHECKLIST: Understanding Electronic Discovery Privilege Waiver Issues.

☐ Review applicable California and federal privilege law addressing:

- ☐ Express waiver;
- ☐ Involuntary disclosure; or
- ☐ Inadvertent disclosure.

Authority:

Evid Code § 950 et seq.; CCP § 2018.030; Fed R Evid 502

Discussion:

See 3.12, 3.13, 3.17

☐ If documents have been produced in federal lawsuit or investigation, determine whether there is an applicable federal court order regarding disclosure.

Authority:

Fed R Evid 502(d)

Discussion:

See 3.17[2]

☐ Review *CCP § 2031.285* clawback rule.

- ☐ Determine if statutory clawback procedure is acceptable.
- ☐ If not, negotiate acceptable non-waiver agreement with opposing counsel.

Authority:

CCP § 2031.285; Cal Rules Ct, Rule 3.724

Discussion:

See 3.14

Form:

Sample clawback provision, see 3.23

- ☐ Keep decisions log to track decision made and steps taken during privilege review.

Authority:

Victor Stanley, Inc. v. Creative Pipe, Inc. (D Md 2008) 250 FRD 251, 255-256

Discussion:

See 3.16[4]

Form:

See *Ch. 5, Initial Procedures in Electronic Discovery--Notice, Document Preparation, Meeting and Conferring, and Case Management Conference*, 5.29.

- ☐ Understand ethical obligations of attorney receiving inadvertently produced privileged ESI.

Authority:

Rico v. Mitsubishi Motors Corp. (2007) 42 C4th 807, 818, 68 CR3d 758 ; State Compensation Ins. Fund v. WPS, Inc. (1999) 70 CA4th 644, 656-657

Discussion:

See 3.15



117 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

IV. UNDERSTANDING ELECTRONIC DISCOVERY PRIVILEGE WAIVER ISSUES

*1-3 MB Practice Guide: CA E-Discovery and Evidence 3.12***AUTHOR:** Diane E. Barry, Esq.**3.12 Options and Strategy When Material Sought in Electronic Discovery May Be Privileged.**

All e-discovery requests should be examined by both the propounding party and the responding party for privilege issues. Review is especially critical for the responding party, as the failure to assert an available claim of privilege in responding to discovery is generally a waiver of the privilege.

If the sheer volume of materials to be produced makes a quick and comprehensive document review for privilege issues impractical, the responding party may assert generally the attorney-client privilege and work product protection, identify the known documents subject to the privilege on a privilege log, and produce all documents then known to be nonprivileged [see, e.g., *United States ex rel. Bagley v. TRW, Inc.* (CD Cal 2001) 204 FRD 170, 172-175 (describing defendant's use of privilege log in review of hundreds of thousands of documents)]. As additional documents are discovered and reviewed, they may then be added to the privilege log or produced as appropriate.

**Strategic Points:**

Privilege protection for ESI is governed by:

- *CCP § 2031.285*, which sets out a framework whereby a producing party can request return of a privileged item.
- Case law, which addresses the ethical obligations of a party who receives a potentially privileged item.
- *Federal Rules of Evidence, Rule 502*, which provides that if a federal court orders that a particular disclosure does not waive privilege, the waiver issue as to those items may not be re-litigated in state court.

**Warning:**

Ethical and practical problems arise when a party opponent attempts to make use of a potentially

privileged item without first settling the issue of its privileged nature. In short, a party may not make use of evidence that is privileged. On the other hand, if the privilege has been waived, a party is free to use that evidence, subject to the rules of relevance and unfair prejudice.

**Strategic Point:**

Counsel must meet and confer [see *Cal Rules Ct., Rule 3.724*]. If the parties are unable to settle the matter among themselves, they may ask the court to determine whether the contested item is privileged. This determination should be made before counsel attempts to use any potentially privileged item.

**Cross References:**

Privilege log, see *Ch. 9, Gathering and Producing Electronically Stored Information*, 9.36-9.46.

Protecting confidentiality and privilege, see *Matthew Bender(R) Practice Guide: California Civil Discovery*, 5.16-5.24.



118 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

IV. UNDERSTANDING ELECTRONIC DISCOVERY PRIVILEGE WAIVER ISSUES

1-3 MB Practice Guide: CA E-Discovery and Evidence 3.13

AUTHOR: Diane E. Barry, Esq.

3.13 California Attorney-Client Privilege and Attorney Work Product Protection.

3.13[1] Attorney-Client Privilege. The attorney-client privilege authorizes a client to refuse to disclose, and to prevent others from disclosing, confidential communications between attorney and client. An attorney has a duty to claim the privilege on the client's behalf [*see Evid Code § 950 et seq.*].

Cross References:

Elements of attorney-client privilege, see *California Forms of Pleading and Practice*, Ch. 191, *Discovery: Privileges and Other Discovery Limitations*, 191.40 *et seq.* (Matthew Bender).

Detailed discussion of attorney-client privilege, see DeMeo, *California Deposition and Discovery Practice*, Ch. 27, *Attorney-Client Privilege* (Matthew Bender).

3.13[2] Attorney Work Product Protection. California's attorney work product doctrine separates an attorney's work into two types. A writing that reflects an attorney's impressions, conclusions, opinions, or legal research or theories is not discoverable under any circumstances. Any other kind of attorney work product is only discoverable, if denial will cause "unfair prejudice" or will result in "injustice" [*CCP § 2018.030* (attorney work product); *Rico v. Mitsubishi Motors Corp.* (2007) 42 C4th 807, 814, 68 CR3d 758].

Cross References:

Elements of attorney work product protection, see *California Forms of Pleading and Practice*, Ch. 191, *Discovery: Privileges and Other Discovery Limitations*, 191.100 *et seq.* (Matthew Bender).

Detailed discussion of attorney work product protection, see DeMeo, *California Deposition and Discovery Practice*, Ch. 28, *Attorney Work Product Protection* (Matthew Bender).

3.13[3] Privileges Are Strictly Construed. As statutory creations, the attorney-client privilege and attorney work product protection are exceptions to the general rule requiring disclosure. Therefore, they are to be strictly construed [*Gonzales v. Municipal Court* (1977) 67 CA3d 111, 118, 136 CR 475] .

► **Cross References:**

Detailed discussion of attorney-client privilege, see DeMeo, *California Deposition and Discovery Practice*, Ch. 27, Attorney-Client Privilege (Matthew Bender).

Detailed discussion of attorney work product protection, see DeMeo, *California Deposition and Discovery Practice*, Ch. 28, Attorney Work Product Protection (Matthew Bender).

3.13[4] Privileges May Be Waived.

3.13[4][a] Waiver Through Voluntary Disclosure. If the client or the client's agent discloses a significant part of a privileged communication, or consents to disclosure by a third party, the privilege is waived. A court considering the subject of waiver must consider both the subjective intent of the client, and any relevant surrounding circumstances that might manifest intent to disclose. [*Evid Code* § 912 (privilege waiver); *State Compensation Ins. Fund v. WPS, Inc.* (1999) 70 CA4th 644, 652, 82 CR2d 799] .

Example:

Corporation discovered improper conduct within its organization, and informed the government that it was willing to share investigation documents subject to a confidentiality agreement. Privileges were waived despite the existence of a confidentiality agreement, as the disclosure was voluntary and not coerced [*McKesson HBOC, Inc. v. Superior Court* (2004) 115 CA4th 1229, 1238-1239, 9 CR3d 812] .

► **Cross References:**

Compelled disclosure, see 3.13[4][b].

Waiver by disclosure or consent to disclosure, see *California Forms of Pleading and Practice*, Ch. 191, *Discovery: Privileges and Other Discovery Limitations*, 191.15[1] (Matthew Bender).

3.13[4][b] Compelled Disclosure Does Not Waive Privilege. Waiver of privilege through disclosure is premised on *voluntary* disclosure, so that if a party is compelled to disclose privileged information, no waiver can be implied from the disclosure [see *Transamerica Computer Co. v. IBM Corp.* (9th Cir 1978) 573 F2d 646, 651-652 (rigorous discovery schedule required by a court order in prior proceedings required party to produce evidence without adequate opportunity for privilege review); *Regents of Univ. of Cal. v. Superior Court* (2008) 165 CA4th 672, 675, 683-684, 81 CR 3d 186] .

Example:

Production of documents to the government by energy suppliers under criminal and regulatory investigation did not waive the attorney-client privilege and work product protection when production was coerced by the threat of indictment if the corporations failed to cooperate [*Regents of Univ. of Cal. v. Superior Court* (2008) 165 CA4th 672, 675, 683-684, 81 CR 3d 186 (*Evid Code* § 919 anticipates that privilege holder will not have to make strenuous efforts to resist disclosure; only reasonable efforts are required)].

► **Cross Reference:**

Compelled disclosure, see DeMeo, *California Deposition and Discovery Practice*, Ch. 27, *Attorney-Client Privilege*, 27.33 (Matthew Bender).

3.13[4][c] Failure to Object Manifests Consent. Consent can be manifested by words or conduct including failure to claim the privilege in any proceeding in which the client has legal standing and opportunity to claim the privilege [*Scottsdale Ins. Co. v. Superior Court* (1997) 59 CA4th 263, 272, 69 CR2d 112 (failure to specifically interpose an

objection on basis of attorney client privilege in formal discovery response waived privilege)].

3.13[4][d] Inadvertent Disclosure Does Not Manifest Consent. Accidental production by an attorney does not manifest consent by the client to disclosure [*Rico v Mitsubishi Motors Corp.* (2007) 42 C4th 807, 810, 68 CR3d 758, 766] .

 Cross Reference:

Inadvertent disclosure, see DeMeo, *California Deposition and Discovery Practice*, Ch. 28, *Attorney Work Product Protection*, 28.04[9] (Matthew Bender).



119 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

IV. UNDERSTANDING ELECTRONIC DISCOVERY PRIVILEGE WAIVER ISSUES

*1-3 MB Practice Guide: CA E-Discovery and Evidence 3.14***AUTHOR:** Diane E. Barry, Esq.**3.14 Inadvertent Disclosure Does Not Constitute Waiver Under CCP § 2031.285 Clawback Rule.**

3.14[1] Clawback Agreement Defined. Parties can minimize the costs and delays of privilege review by entering into "clawback," or nonwaiver, agreements, under which inadvertently produced material is returned without waiver [see Judicial Council of California Invitation to Comment, Note 6 (*CCP* § 2031.285)].

**Strategic Point:**

Clawback agreements are prevalent in large-scale document matters in which the sheer number of items makes inadvertent production likely. To preserve privileges, California law requires that a party have taken reasonable precautions under the circumstances. A clawback agreement meets this requirement. Clawback agreements preserve a privilege when it would otherwise have been waived. Under the prototypical clawback agreement, the producing party agrees to conduct the best privilege review it can, given the time constraints of the matter and the bulk of materials to be reviewed and produced. Privileged documents that are inadvertently disclosed are returned to the producing party.

**Warning:**

"Quick peek" agreements are not clawback agreements. A "quick peek" agreement may not meet the requirements of *CCP* § 2031.285. A quick peek agreement typically permits the opposing counsel to take a quick look at the bulk corpus of documents and to identify the documents to be produced. Counsel then conducts a privilege review only of those documents. Since precautions were not taken in advance of permitting opposing counsel to review the documents, this process may not protect against waiver [see, e.g., *Hartford Fire Ins. Co. v. Garvey* (*ND Cal* 1985) 109 *FRD* 323, 332 (attorney-client privilege and work product protection were waived when opposing counsel was permitted to review and copy documents brought to deposition before producing counsel reviewed them and noticed that privileged items were included)]. The better practice is to have the judge specify in the case management order how the document review will be conducted. In these circumstances, it is unlikely that a judge will later determine that the review procedure was unreasonable.

► Cross References:

CCP § 2031.285 Clawback Rule, see *California Forms of Pleading and Practice*, Ch. 195A, *Discovery: Discovery of Electronically Stored Evidence (E-Discovery)*, § 195A.21§ 195A.31, § 195A.56 (Matthew Bender).

3.14[2] Clawback Rule Applies Only to Inadvertent Production of Electronically Stored Information. By its terms, CCP § 2031.285 applies *only* to the inadvertent production of privileged ESI. It does not apply to the inadvertent production of other privileged materials [CCP § 2031.285(a)].

3.14[3] Clawback Rule Does Not Create New Rights. CCP § 2031.285 does not create any new rights or privileges. Instead, CCP § 2031.285 formalizes the existing process for reclaiming inadvertently produced privileged ESI and sets out timing for each step [CCP § 2031.285; cf. *State Compensation Ins. Fund v. WPS, Inc.* (1999) 70 CA4th 644, 82 CR2d 799 (inadvertent disclosure pre-CCP § 2031.285)].

3.14[4] Clawback Rule May Be Modified by Parties. Parties may make their own stipulations if the provisions of CCP § 2031.285 do not meet their needs [see Judicial Council of California Invitation to Comment, Note 6 (CCP § 2031.285)]. Counsel may also agree to alternative inadvertent production arrangements addressing confidentiality and privilege protections, and these can be made part of the case management order [see *Cal Rules Ct, Rule 3.728(13)*; *Cal Rules Ct, Rule 3.724(8)(F)*].

Example:

The parties entered into a complex stipulation regarding protocols for e-discovery and clawback of privileged materials. Their agreement was formalized by the court and entered as an order. One of the parties challenged a privilege claim after the timing for challenges contained in the stipulation and the court order had passed. The court denied the challenge on the ground that the terms of the stipulation and the order were dispositive [*Bro-Tech Corp. v. Thermax, Inc.* (2008 ED Pa) 2008 US Dist LEXIS 100749, at *8] .

3.14[5] Clawback Rule Does Not Decide Substantive Privilege Issues. CCP § 2031.285 provides no guidance on the substantive issues of privilege law. It does not address how to assess the legitimacy of privilege claims, or what constitutes "waiver," "consent," or "inadvertence" [CCP § 2031.285; see *Hartford Fire Ins. Co. v. Garvey* (ND Cal 1985) 109 FRD 323, 332 (applying prior case law to issue of "inadvertence" under *Fed R Evid 502*)].

3.14[6] Clawback Rule Creates Framework for Producing Party to Reclaim Inadvertently Produced Materials.

3.14[6][a] Actions Are Specified From Perspective of Producing Party. CCP § 2031.285 is drafted from the perspective of the producing party who discovers that it has produced a privileged item. The provision lists the steps the producing party must take in order to reclaim the privileged material [see CCP § 2031.285]. This approach differs from that taken in pre-existing case law, which addresses the issue of inadvertent production from the perspective of the receiving party [see, e.g., *State Compensation Ins. Fund v. WPS, Inc.* (1999) 70 CA4th 644, 656-657, 82 CR2d 799 (providing standard for attorney conduct on receipt of inadvertently disclosed privileged matter)].

► Cross References:

Form for notice to receiving attorney regarding inadvertent production of privileged materials, see 3.23.

Waiver through inadvertent discovery generally, see DeMeo, *California Deposition and Discovery Practice*, Ch. 27, *Attorney-Client Privilege*, 27.34 (Matthew Bender).

3.14[6][b] Notice to Receiving Party. If ESI produced in discovery is subject to a claim of privilege or protection, the producing party must send notice to all receiving parties.

**Timing:**

Receiving party has 30 days to challenge the privilege classification; see 3.14[6][e].

3.14[6][c] Contents of Notice. The notice must specify the items deemed privileged and the basis for the privilege claim [CCP § 2031.285(a)].

**Cross Reference:**

Form for notice to receiving attorney regarding inadvertent production of privileged materials, see 3.24.

3.14[6][d] Receiving Party Must Take Reasonable Steps to Sequester Identified Items. On receipt of the notice from the producing party, the receiving party must take immediate reasonable steps to "sequester" the items identified. If the materials have been provided to experts or other personnel outside the receiving party, the receiving party must take reasonable steps to reclaim the materials. Until the question of privilege is settled, the receiving party may not make any use of the identified items [CCP § 2031.285(b)-(d); see *State Compensation Ins. Fund v. WPS, Inc.* (1999) 70 CA4th 644, 656-657 ; 82 CR2d 799 (receiving parties must sequester, reclaim, and not use potentially privileged materials, decided under prior law)].

3.14[6][e] Receiving Party Has 30 Days to Challenge Privilege Classification. The receiving party has 30 days from receipt of the CCP § 2031.285(a) notice to decide whether to challenge the claim of privilege. To challenge the privilege claim, a motion must be filed within 30 days from receipt of the notice, presenting the challenged items to the court under seal [CCP § 2031.285(d)].

**Strategic Points:**

- The 30-day time frame for the receiving party to challenge the attempt to reclaim begins with receipt of this notice [see CCP § 2031.285[d][1]]. Consider using a messenger service or overnight delivery method to send out the notice, and keep proof of delivery.
- If the receiving party decides not to challenge the privilege designation, common practice is to provide producing counsel with a certification that the ESI in question has been wiped or otherwise eradicated.

**Cross Reference:**

Form for motion to challenge claim of privilege, see *California Forms of Pleading and Practice*, Ch. 195A, *Discovery: Discovery of Electronically Stored Evidence (E-Discovery)*, §195A.63 (Matthew Bender).



120 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

IV. UNDERSTANDING ELECTRONIC DISCOVERY PRIVILEGE WAIVER ISSUES

1-3 MB Practice Guide: CA E-Discovery and Evidence 3.15

AUTHOR: Diane E. Barry, Esq.

3.15 Ethical Obligations of Attorney Receiving Inadvertently Produced Privileged Electronically Stored Evidence.

3.15[1] CCP § 2031.285 Leaves Untouched Attorney's Pre-Existing Obligations. *CCP § 2031.285* applies only to the inadvertent production of privileged ESI. It makes no attempt to overrule or otherwise alter the pre-existing ethical obligations of counsel who receive potentially privileged items of any kind [*CCP § 2031.285(a)*].

Cross Reference:

Duty to maintain client confidences and secrets, see *California Forms of Pleading and Practice*, Ch. 72, *Attorney Practice and Ethics*, 72.33 (Matthew Bender).

3.15[2] Attorney's Obligations Are Ethical Rather Than Statutory. Prior to the enactment of *CCP § 2031.285*, the duties and obligations in the area of inadvertent privilege production were addressed in case law, and from the perspective of the receiving party. These duties were stated in terms of the ethical obligations of counsel to other counsel and the judicial system [*Rico v. Mitsubishi Motors Corp.* (2007) 42 C4th 807, 818, 68 CR3d 758 (attorney disqualified for making use of attorney work product privileged materials after privileged nature was ascertained by him, adopting rule set out in *State Compensation Ins. Fund v. WPS, Inc.* (1999) 70 CA4th 644, 656-657, 82 CR2d 799)].

Cross Reference:

Ethical duty of attorney who receives inadvertent disclosure, see Ch. 191, *Discovery: Privileges and Other Discovery Limitations*, 190.24[8], 191.15[7][b].

3.15[3] Attorney's Ethical Obligations Arise As Soon As It Is Reasonably Apparent That Evidence Is Privileged. The attorney is under an obligation to review only so much of the document as is necessary to ascertain its privileged nature. As soon as it is reasonably apparent that the material is potentially privileged, and therefore was inadvertently produced, the attorney is obligated to cease review of the material [*Rico v. Mitsubishi Motors Corp.* (2007) 42 C4th 807, 815-819, 68 CR3d 758 (attorney was disqualified for making use of attorney work product privileged materials after he has ascertained their privileged nature)].

3.15[4] Attorney Should Quarantine Potentially Privileged Items. Although case law does not impose a specific ethical obligation to quarantine potentially privileged items or to retrieve them from others to whom they were disseminated, the California Supreme Court has upheld the disqualification of experts who reviewed and used privileged materials. While the experts had not committed any affirmative bad act, their exposure to the privileged documents required their disqualification [*Rico v. Mitsubishi Motors Corp.* (2007) 42 C4th 807, 815-819, 68 CR3d 758] .



Strategic Point:

Pending settlement of the privilege issues, counsel should quarantine potentially privileged items and take reasonable steps to retrieve them from any experts or other support personnel to whom they were disseminated. Counsel should also document the extent of his or her exposure to those items.

3.15[5] Attorney's Ethical Obligation to Notify Producing Counsel. Once an attorney identifies an item produced as potentially privileged, he or she must immediately notify the producing party's counsel [*Rico v. Mitsubishi Motors Corp.* (2007) 42 C4th 807, 815-819, 68 CR3d 758] .

3.15[6] Attorney's Obligation to Settle Privilege Issues. After notifying the producing party, the parties then may proceed to resolve the situation by agreement or may resort to the court for guidance, with the benefit of protective orders and other judicial intervention [see *State Comp. Ins. Fund v. WPS, Inc.* (1999) 70 CA 4th 644, 656-657, 82 Cal. Rptr. 2d 799] .



Strategic Point:

It is good practice to file motions asking the court to settle privilege issues under seal. Requiring that these motions be filed under seal can be made part of the case management order under *Cal Rules Ct, Rule 3.724*. However, even without its incorporation in the case management order, the better practice is still to file under seal, given the stricture for filing potentially privileged items under seal in *CCP § 2031.285*--despite the fact that case law does not specifically require it. Counsel should keep in mind that attorneys have an ethical obligation to each other and to the judicial system as a whole to act appropriately to preserve issues of privilege for proper resolution.



121 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

IV. UNDERSTANDING ELECTRONIC DISCOVERY PRIVILEGE WAIVER ISSUES

1-3 MB Practice Guide: CA E-Discovery and Evidence 3.16

AUTHOR: Diane E. Barry, Esq.

3.16 Privilege Issues That May Arise As Result of Using Computer Technology for Privilege Review.

3.16[1] Waiver Concerns. The sheer volume of ESI makes the task of privilege review more difficult than it has been in the past [Judicial Council of California Invitation to Comment, p. 2]. One of the more useful properties of ESI is that it is searchable. Computer tools can be used to speed the privilege review [see, e.g., *Victor Stanley, Inc. v. Creative Pipe, Inc.* (D Md 2008) 250 FRD 251, 256-257, 259-261 (extensive discussion of literature explaining keyword search techniques, their deficiencies and limitations)]. However, computer technologies also add new shoals to be navigated by the discovery practitioner. If short cuts are taken, waiver can occur [see, e.g., *Rhoads Indus. v. Bldg. Materials Corp. of Am.* (ED Pa 2008) 254 FRD 216, 222-223 (plaintiff failed to prepare for segregation and review of privileged documents sufficiently far in advance of inevitable production of large volume of documents)].

Example:

Defendants failed to demonstrate that the keyword search they performed on the text-searchable electronically stored information was reasonable. They neither identified the keywords selected nor the qualifications of the persons who selected them to design a proper search; they failed to demonstrate that there was quality assurance testing; they failed to carry their burden of explaining what they had done and why it was sufficient; and they voluntarily abandoned their request for a court-approved non-waiver agreement. Because defendants did not take reasonable precautions to prevent the disclosure of privileged information, any privilege or protection was waived by defendants' voluntary production of the documents [see *Victor Stanley, Inc. v. Creative Pipe, Inc.* (D Md 2008) 250 FRD 251, 262] .



Cross Reference:

Waiver issues particular to e-discovery, see *California Forms of Pleading and Practice Ch. 195A, Discovery: Discovery of Electronically Stored Evidence (E-Discovery)*, § 195A.17 (Matthew Bender).

3.16[2] Search Methodology. Privilege review methods, including computerized search methods, must be reasonable under the circumstances, or waiver may occur. Selection of appropriate search methodology to identify privileged materials requires careful planning and testing to show that search methodology employed actually returns the target items desired [*Victor Stanley, Inc. v. Creative Pipe, Inc.* (D Md 2008) 250 FRD 251, 262 (defendants offered no proof of quality control testing of methodology employed or other proof that terms selected actually returned

privileged items)].



Cross Reference:

Obtaining evidence about how ESI is maintained, see *Matthew Bender(R) Practice Guide: California Civil Discovery*, 5.08.

3.16[3] Participant Qualifications. Computer queries intended to isolate privileged materials must be designed by persons qualified to design effective search protocols [*Victor Stanley, Inc. v. Creative Pipe, Inc. (D Md 2008) 250 FRD 251, 259-260* (proof that search terms were selected by two attorneys, without more, was not sufficient to prove that qualified personnel had designed search methodology); see *United States v. O'Keefe (DDC 2008) 537 F Supp2d 14, 24* ("[w]hether search terms or 'keywords' will yield the information sought is a complicated question involving the interplay, at least, of the sciences of computer technology, statistics and linguistics")].

3.16[4] Documentation and Proof. An attorney must both use appropriate computer tools and technologies, and be able to prove that appropriate tools and technologies were used [*Victor Stanley, Inc. v. Creative Pipe, Inc. (D Md 2008) 250 FRD 251, 261-262* (defendants failed to prove that their privilege review methodology was reasonable under the circumstances; burden lies with party claiming privilege)].



Strategic Point:

Counsel should keep a "decisions log" that lists all privilege decisions, the dates on which they were made, the rationale for each decision, the name of the decision maker, and his or her qualifications. A basic spreadsheet can be used to keep this essential information for later use.



Cross Reference:

Form for privilege log, see *Ch. 9, 9.46*.



122 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

IV. UNDERSTANDING ELECTRONIC DISCOVERY PRIVILEGE WAIVER ISSUES

1-3 MB Practice Guide: CA E-Discovery and Evidence 3.17

AUTHOR: Diane E. Barry, Esq.

3.17 Role of Federal Rule 502 in State Court Matters Involving Attorney-Client Privilege and Work Product.

3.17[1] Overview of Federal Rule 502 Concerns Effect of Attorney-Client and Work Product Privileges. *Fed R Evid 502* is a federal rule of evidence concerning the effect of the disclosure of materials protected by attorney-client privilege or attorney work product protection. The rule addresses:

- The existence of a waiver of privilege due to disclosure of the privileged or work product material;
- The scope of any waiver (whether a waiver is limited to particular disclosed materials, or extends to all materials related to the same subject matter); and
- How disclosures before different federal and/or state proceedings will be subsequently treated.

Although the rule is primarily concerned with federal court proceedings, it does apply, in limited circumstances, to state court proceedings.



Cross References:

Effect of *Fed R Evid 502* on state court proceedings, see 3.17[2].

Detailed discussion of *Fed R Evid 502*, see Weinstein's Federal Evidence, Ch. 502, Attorney-Client Privilege and Work Product; Limitations on Waiver (Matthew Bender 2d ed.).

3.17[2] Effect of Federal Rule 502 on State Court Proceedings. *Fed R Evid 502* is more than a federal judicial rule—it was passed as an act of Congress and is binding on state courts. The rule is binding on any state court in which parties wish to introduce previously disclosed materials and litigate the waiver issues based upon the earlier production in federal court [*Fed R Evid 502(f)*; Advisory Committee Note].

With respect to state court actions, *Fed R Evid 502* affects state court proceedings as follows:

■ In determining whether a disclosure in a federal proceeding or to a federal agency waived the privilege for the disclosed material, a state court should find no waiver if (1) the disclosure was inadvertent; (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and (3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following *Fed R Civ P 26(b)(5)(B)* [*Fed R Evid 502(b)*].

■ When a waiver exists due to a disclosure in a federal proceeding or to a federal agency, a state court should find no waiver of privilege as to the *undisclosed* materials unless (1) the waiver is intentional; (2) the disclosed and undisclosed communications or information concern the same subject matter; and (3) they ought in fairness to be considered together [*Fed R Evid 502(a)*].

■ When a federal court has ordered that a disclosure in a federal court proceeding is not a waiver in the litigation then pending before the federal court, a state proceeding may not re-litigate that issue [*Fed R Evid 502(d)*].

■ When the disclosure has been made in a state proceeding and is not subject to a state court order concerning waiver, a federal court will not find waiver if the disclosure would not have been a waiver under either *Fed R Evid 502* or the state's law of waiver [*Fed R Evid 502(c)*].

■ An agreement between the parties as to disclosure in a federal proceeding is binding only on the parties to the agreement unless it is incorporated into a court order [*Fed R Evid 502(e)*].

➤ **Cross Reference:**

Inadvertent disclosure in state proceeding, see *Weinstein's Federal Evidence, Ch. 502, Attorney-Client Privilege and Work Product; Limitations on Waiver, 502.05* (Matthew Bender 2d ed.).

3.17[3] Federal Rule 502 Applies in Limited Circumstances. *Fed R Evid 502* applies only to disclosure of materials protected by the attorney-client privilege and work product. Further, the rule governs waiver of the attorney-client privilege and work product protection only in the specific situations listed in the rule [*Fed R Evid 502; Advisory Committee Note*].

➤ **Cross Reference:**

Purpose and applicability of *Fed R Evid 502*, see *Weinstein's Federal Evidence, Ch. 502, Attorney-Client Privilege and Work Product; Limitations on Waiver, 502.02* (Matthew Bender 2d ed.).



123 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

V. ATTORNEY'S ETHICAL DUTIES REGARDING E-DISCOVERY UNDER THE CALIFORNIA CODE OF PROFESSIONAL CONDUCT

1-3 MB Practice Guide: CA E-Discovery and Evidence 3.18

AUTHOR: Diane E. Barry, Esq.

3.18 CHECKLIST: Attorney's Ethical Duties Regarding E-Discovery Under the California Code of Professional Conduct.

☐ Assess attorney's technical skill level with respect to e-discovery, keeping in mind that:

☐ Attorney must act competently in performing legal services.

☐ Attorney must protect client confidences from disclosure.

Authority:

Cal Rules Prof Conduct, Rule 3-110; Victor Stanley, Inc. v. Creative Pipe, Inc. (D Md 2008) 250 FRD 251, 259-260

Discussion:

See 3.19, 3.20-3.21

☐ Review relevant sections of Cal Rules Prof Conduct to ensure attorney's understanding of his or her ethical obligations in conducting e-discovery.

Authority:

Cal Rules Prof Conduct, Rules 1-100, 3-110

Discussion:

See 3.19-3.21



124 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

V. ATTORNEY'S ETHICAL DUTIES REGARDING E-DISCOVERY UNDER THE CALIFORNIA CODE OF PROFESSIONAL CONDUCT

1-3 MB Practice Guide: CA E-Discovery and Evidence 3.19

AUTHOR: Diane E. Barry, Esq.

3.19 Options and Strategy.

Before accepting an engagement that requires e-discovery skills, the attorney should assess whether he or she has the requisite technical skills, and if not, whether the attorney can retain someone who can provide this expertise [*see Cal Rules Prof Conduct, Rule 3-110* (failing to act competently)]. The California Rules of Professional Conduct provide a roadmap of issues that are likely to be implicated in the attorney's decision.

► **Cross References:**

Duty to act competently in e-discovery, see 3.21.

Duty of competence generally, see *California Forms of Pleading and Practice, Ch. 72, Attorney Practice and Ethic, 72.270* (Matthew Bender).



125 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

V. ATTORNEY'S ETHICAL DUTIES REGARDING E-DISCOVERY UNDER THE CALIFORNIA CODE OF PROFESSIONAL CONDUCT

1-3 MB Practice Guide: CA E-Discovery and Evidence 3.20

AUTHOR: Diane E. Barry, Esq.

3.20 Remedies and Sanctions in Rules of Professional Conduct Are Not Exclusive.

The remedies and sanctions contained in the California Rules of Professional Conduct are not exclusive. The same conduct can be subject to multiple regulations and penalties [*Cal Rules Prof Conduct, Rule 1-100(A)*].

Examples:

Signing a false certification or affidavit is:

- An ethical violation under *Cal Rules Prof Conduct, Rule 5-220* (suppression of evidence), and *B&P Code § 6068* (attorney's duties).
- A discovery abuse subject to sanctions under *CCP § 2023.010(e), (f)*.
- A criminal act of perjury [*Pen Code § 118a* (false affidavit is perjury)].



Cross Reference:

Types of sanctions available for discovery misuse; motions seeking and opposing sanctions, see *Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 3, Sanctions, 3.10-3.14*.



126 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

V. ATTORNEY'S ETHICAL DUTIES REGARDING E-DISCOVERY UNDER THE CALIFORNIA CODE OF PROFESSIONAL CONDUCT

1-3 MB Practice Guide: CA E-Discovery and Evidence 3.21

AUTHOR: Diane E. Barry, Esq.

3.21 Attorneys Must Act Competently When Performing Legal Services.

An attorney has a duty to act competently in any engagement for legal services. Competence includes diligence and any learning and skill that is required for the engagement. In order to accept an engagement that requires special skills, counsel need not have all of those skills at the outset of the engagement. Rather, an attorney may learn what he or she needs to know along the way, provided that learning takes place in time for the acquired skill to be used when needed in the engagement. An attorney also may associate with another lawyer or expert who has the necessary competencies [see *Cal Rules Prof Conduct, Rule 3-110*].

Consider:

The rule requiring competency has particular application to e-discovery. In these cases, competency must include e-competency. A law degree is not sufficient to provide counsel with all skills required in the e-discovery context [see, e.g., *Victor Stanley, Inc. v. Creative Pipe, Inc. (D Md 2008) 250 FRD 251, 259-260* (proof that search terms were selected by two attorneys without more was not sufficient to prove that qualified personnel had designed search methodology)].



Cross Reference:

Duty of competence generally, see *California Forms of Pleading and Practice, Ch. 72, Attorney Practice and Ethic, 72.270* (Matthew Bender).



127 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

V. ATTORNEY'S ETHICAL DUTIES REGARDING E-DISCOVERY UNDER THE CALIFORNIA CODE OF PROFESSIONAL CONDUCT

1-3 MB Practice Guide: CA E-Discovery and Evidence 3.22

AUTHOR: Diane E. Barry, Esq.

3.22 Attorneys Must Protect Client's Confidential Information From Disclosure.

Failure to protect a client's confidential and privileged information from disclosure is both an ethical violation and grounds for disbarment [*B&P Code §§ 6068(e)(1), 6103; Cal Rules Prof Conduct, Rule 3-100*]. When an engagement requires discovery of ESI and the use of computerized tools to conduct privilege review, an attorney who is not familiar with those tools and protocols must gain that competency or must associate with someone who is competent to assist in that area [*see, e.g., Victor Stanley, Inc. v. Creative Pipe, Inc. (D Md 2008) 250 FRD 251, 259-260* (proof that search terms were selected by two attorneys without more was not sufficient to prove that qualified personnel had designed search methodology)].



Cross Reference:

Duty to maintain client confidences and secrets, see *California Forms of Pleading and Practice, Ch. 72, Attorney Practice and Ethic, 72.33* (Matthew Bender).



128 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery

VI. FORMS

1-3 MB Practice Guide: CA E-Discovery and Evidence 3.23

AUTHOR: Diane E. Barry, Esq.

3.23 Clawback Provision.

Clawback Provision.

_____. Inadvertent Production.

The parties acknowledge the large number of documents and electronically stored information (ESI) to be reviewed and produced in this proceeding. The parties are entering into this stipulation in order to move this evidence production forward quickly, so that the case may proceed without the delay that would result if each party were to conduct an in-depth privilege and responsiveness review. However, the parties acknowledge the each party's right to protect any privileged information in the documents and ESI under review in this proceeding. Accordingly, the parties agree that the privilege review in this matter will be conducted as follows: _____ [describe how privilege review will be conducted].

In the event that privileged documents or ESI are inadvertently produced by any party to this proceeding, the party may, within a reasonable period of time, request that the document or ESI be returned. For each item claimed to be privileged, the request must include a description the item, a designation of the privilege claimed, and the basis for the privilege claim.

After being notified, the receiving party must promptly _____ [return, sequester, or destroy] the specified items and any copies, and may not use or disclose the information until the claim is resolved. If the receiving party has disclosed the information before being notified of its privileged status, the receiving party must take reasonable steps to retrieve it. The producing party must preserve the information until the claim is resolved. The receiving party may present the information to the court under seal for a determination of the privilege claim within a reasonable time after receipt of the notice claiming privilege.

NOTES:

Authority:

CCP § 2031.285

► **Cross References:**

CCP § 2031.285 clawback rule, see 3.14; attorney-client privilege and work product protection, see 3.13



129 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 3 Ethical Issues for Attorneys in E-Discovery
VI. FORMS*1-3 MB Practice Guide: CA E-Discovery and Evidence 3.24***AUTHOR:** Diane E. Barry, Esq.**3.24 Notice to Receiving Counsel Regarding Inadvertent Production of Privileged Electronically Stored Information.**Notice to Receiving Counsel Regarding Inadvertent Production of Privileged Electronically Stored Information.
[date]

[attorney's name and California Bar number]

[attorney's street address]

[city, state, and ZIP code]

[telephone number]

[fax number]

[e-mail address]

Attorney for [party's status and name]

Dear _____ [attorney for opposing party]:

RE: _____ v. _____, Case No. _____

Notification of Inadvertent Production of Privileged ESI

This letter is being sent to you in accordance with *CCP* § 2031.285(a) to notify you of an inadvertent production of privileged electronically stored information (ESI) to your client in the above captioned matter. We hereby request the immediate return [or certified destruction] of the following privileged items:

Control No.	Privilege Asserted	Basis for Privilege Claim
ABC_0000001	Attorney Client Privileged	[e.g., E-mail communication between _____ [client] and in-house legal staff dated _____]
ABC_0008943	Attorney Work Product	[e.g., Attorney notes from _____ (specify) dated _____]

These privileged items were produced to you on _____ [date] in response to your discovery request in this matter.

If you have any questions or concerns regarding this notification, please do not hesitate to contact me.

Sincerely,

[firm name]

By: _____ [signature of attorney]

[attorney name]

NOTES:

Authority:

CCP § 2031.285



Cross References:

CCP § 2031.285 clawback rule, see 3.14; attorney-client privilege and work product protection, see 3.13



130 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 4 Planning E-Discovery

1-4 MB Practice Guide: CA E-Discovery and Evidence 4.syn

AUTHOR: Steve Williams

§ 4.syn Synopsis to Chapter 4: Planning E-Discovery

4.01 Scope.

4.02 Objective and Strategy.

4.03 CHECKLIST: Determining Use and Extent of E-Discovery in Case.

4.04 Options and Strategies.

4.05 Counsel Must Assess Need for E-Discovery.

4.05[1] Counsel Must Determine Importance of ESI in Case.

4.05[2] Nearly Every Case Involves ESI.

4.05[3] Counsel Should Not Assume That E-Discovery Is Not Feasible.

4.06 Counsel Must Determine Potential Scope of E-Discovery in Particular Case.

4.06[1] Subject Matter and Location of ESI Should Be Considered.

4.06[2] Extent of E-Discovery Will Depend on Nature of Case.

4.06[3] Nature of Parties and Witnesses Will Play Major Role in Determining Scope of E-Discovery.

4.07 Counsel Should Evaluate Advantages and Benefits of E-Discovery.

4.07[1] ESI Can Be Essential to Win Case.

4.07[2] E-Discovery Can Result in More Focused Discovery.

4.07[3] E-Discovery Can Facilitate Better Case Management Planning.

4.08 Attorney Should Evaluate Challenges of E-Discovery.

4.08[1] Attorney May Have to Learn New Technology and Procedures.

4.08[2] E-Discovery Presents Timing Challenges.

4.08[2][a] Counsel Must Develop Working Knowledge of Terminology and ESI Production Prior to "Meet and Confer" Meeting.

4.08[2][b] Counsel Must Identify Key Custodians Early in Process.

4.08[2][c] Counsel Must Decide on Search Methods Early in Process.

4.08[2][d] Use of E-Discovery Can Increase Overall Discovery Time.

4.08[3] Consultants or Experts Are Often Necessary.

4.08[4] Counsel Must Consider Potential Cost of E-Discovery.

4.08[4][a] E-Discovery Can Be Extremely Expensive.

4.08[4][b] Counsel Must Evaluate Potential for Cost-Shifting to Requesting Party.

4.09 Counsel Should Learn About ESI From Responding Party.

4.09[1] Learning About Responding Party's Electronic Systems Is Essential.

4.09[2] Other Party's Document Storage and Retention Policies Should Be Investigated.

4.09[3] Changes in Respondent's Software or Data Storage Platforms Should Be Identified.

4.09[4] Specialized Programs Should Be Addressed.

4.09[5] Respondent's Key Custodians for the Parties Should Be Identified.

4.10 Counsel Should Consider What Format to Request.

4.10[1] Native Format.

4.10[2] TIFF Format.

4.10[3] Metadata.

4.11 CHECKLIST: Evaluating and Obtaining Expert Assistance.

4.12 Options and Strategies.

4.13 Counsel Should Determine What Role E-Discovery Experts Will Play.

- 4.13[1] Educating Counsel.
- 4.13[2] Educating Client.
- 4.13[3] Educating Court.
- 4.13[4] Participating in Conferences of Counsel Regarding E-Discovery Issues.
- 4.13[5] Assisting in Formulating Discovery Plan.
- 4.13[6] Collecting E-Discovery and Maintaining Chain of Custody.
- 4.13[7] Filtering or Narrowing the Population.
- 4.13[8] Privilege Review.
- 4.13[9] Forensic Data Recovery.
- 4.13[10] Hosting and Managing Production.
- 4.13[11] Confidential Information, Proprietary Databases, and Unique Data.
- 4.14 Choosing an E-Discovery Vendor.
- 4.14[1] Types of Vendors.
- 4.14[2] Vendors Can Assist in Connection With Litigation Hold.
- 4.14[3] Vendors Can Perform Identification and Collection Tasks.
- 4.14[4] Vendors Will Perform Review and Analytics.
- 4.14[5] E-Mail and Content Archiving and Management.
- 4.14[6] Enterprise Content and Records Management.
- 4.14[7] Litigation Support Database.
- 4.15 CHECKLIST: Budgeting for E-Discovery.
- 4.16 Options and Strategies.
- 4.17 Elements of an E-Discovery Budget.
- 4.17[1] Summary of Principal Budget Components.
- 4.17[2] Preservation.
- 4.17[3] Collection.
- 4.17[4] Processing.

4.17[5] Review.

4.17[6] Production.

4.17[7] Privilege Log.

4.17[8] Example of Total Budget.

4.18 Counsel Should Seek Limiting Discovery to Save Avoidable Expense.

4.18[1] Counsel Should Consider Whether Costs Outweigh Benefits.

4.18[2] Early Negotiations Can Limit Scope and Cost of E-Discovery.

Steve Williams n*

FOOTNOTES:

(n7)Footnote *. Steve Williams is a partner with Cotchett, Pitre & McCarthy, Burlingame, California. He practices exclusively in the fields of litigation, trial, and client counseling. He was a member of the California Discovery Subcommittee for revision of California discovery rules and statutes relating to electronic discovery and electronically stored information, 2007-2008, and in that capacity participated in developing the Judicial Council proposal that ultimately became the Electronic Discovery Act. He is admitted to practice in California, New York, and New Jersey, and speaks frequently on discovery and e-discovery issues.



131 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 4 Planning E-Discovery

I. STRATEGY

1-4 MB Practice Guide: CA E-Discovery and Evidence 4.01

AUTHOR: Steve Williams

4.01 Scope.

This chapter describes the key aspects of e-discovery that practitioners must understand in order to prepare a discovery plan for the discovery of electronically stored information (ESI). This includes:

- How to determine what e-discovery is necessary and appropriate [see 4.05].
- The use of consultants or outside vendors to assist with e-discovery [see 4.13].
- Budgeting for e-discovery [see 4.13].
- The ways in which e-discovery issues will affect the timing and scope of discovery [see 4.09].



Core Statutes:

CCP § 2016.010 et seq.



132 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 4 Planning E-Discovery

I. STRATEGY

1-4 MB Practice Guide: CA E-Discovery and Evidence 4.02

AUTHOR: Steve Williams

4.02 Objective and Strategy.

An attorney involved in civil litigation in California state courts must understand the importance and use of e-discovery in the context of that litigation, and be in a position to effectively handle the critical e-discovery tasks necessary for effective representation of clients. Because it is essential to bring these skills to bear from the outset of litigation, this chapter identifies the key preliminary matters that must be addressed so that a practitioner will be able to:

- Counsel a client about its own discovery obligations.
- Prepare a discovery plan.
- Participate in meetings of counsel concerning e-discovery issues.
- Execute a discovery plan that properly addresses e-discovery.

Because California's Electronic Discovery Act, which became effective June 29, 2009, has similarities to federal law, reference is made to federal precedent as federal authorities may provide guidance in construing California law.

The primary strategic considerations forming the theme of this chapter are reasonableness and a weighing of the need for information against the cost and burden involved in retrieving the information. Counsel who has developed the ability to plan for e-discovery with these principles in mind will earn greater credibility in the eyes of the court, other counsel, and the parties.



Strategic Point--Educate the Client:

At the outset, counsel should explain to the client the role that e-discovery will play in the case. This includes explaining document preservation and e-discovery obligations at an early point, as well as the anticipated searches for and productions of documents that all parties will be obligated to make and the costs that are anticipated. Counsel should consider documenting that explanation with a letter to the client to ensure that the information is clearly communicated and there is less chance for a misunderstanding. Care in these early communications, particularly as to planning and responsibility for

adequate preservation and searches, is important because failure to produce discoverable ESI can lead to sanctions for both client and lawyer [see, e.g., *Qualcomm Inc. v. Broadcom Corp.* (SD Cal January 7, 2008) 2008 US Dist LEXIS 911] .

Detailed Discussion/Forms:

California Forms of Pleading and Practice, Ch. 195, Discovery: Inspection of Tangible Evidence (Matthew Bender).

DeMeo, California Deposition and Discovery Practice, Ch. 61, Demand for Inspection of Documents, Things, and Land (Matthew Bender).

Matthew Bender(R) Practice Guide: Federal Pretrial Civil Procedure in California, Ch. 23, Methods of Discovery, Part VII, Discovery of Electronically Stored Information.

Moore's Federal Practice, Ch. 37A, Discovery of Electronically Stored Information.

Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 5, Discovery of Electronic Evidence (Matthew Bender).



133 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 4 Planning E-Discovery

II. DETERMINING USE AND EXTENT OF E-DISCOVERY IN CASE

1-4 MB Practice Guide: CA E-Discovery and Evidence 4.03

AUTHOR: Steve Williams

4.03 CHECKLIST: Determining Use and Extent of E-Discovery in Case.

☐ Assess need for e-discovery.

☐ Determine whether ESI is likely to affect case.

☐ Are there likely to be e-mails relevant to case?

☐ Are documents relevant to case likely to be stored on a computer or other ESI storage media?

☐ Are other electronic records (e.g., cell phone call logs) likely to affect issues in case?

Discussion:

See 4.06

☐ Determine how much e-discovery is likely to be needed.

☐ How much information relevant to the litigation is likely to exist?

☐ Where is that information likely to reside, e.g.:

☐ Computer networks.

- ☐ Servers.
- ☐ Desktop computers.
- ☐ Laptop computers.
- ☐ Cell phones.
- ☐ Blackberries.
- ☐ Personal data assistants (PDAs).
- ☐ Flash drives.
- ☐ Memory sticks and cards.
- ☐ Printers.

Discussion:

See 4.06[1]

- ☐ Is ESI a central or peripheral element of case?

Discussion:

See 4.06[2]

- ☐ How many parties and witnesses are potentially in possession of relevant ESI?

- ☐ Are those parties entities, and if so, how large are they?

Discussion:

See 4.06[3]

- ☐ Evaluate advantages and disadvantages of e-discovery.

- ☐ Advantages:

- ☐ ESI can be essential or critical to winning case.
- ☐ ESI can result in more focused discovery.

- ☐ E-discovery can facilitate better case management planning.

Discussion:

See 4.07

☐ Challenges:

- ☐ May involve learning new technology and procedures.
- ☐ Will require careful attention to timing early in process.
- ☐ May increase overall discovery time.
- ☐ Often requires participation of consultants or experts.
- ☐ Can be expensive.
- ☐ Can potentially result in shifting of all or part of respondent's discovery costs to requesting party.

Authority:

CCP § 2031.280(e) (cost shifting)

Discussion:

See 4.08

- ☐ As soon as possible, learn as much as possible about responding party, including:

- ☐ Responding parties' electronic systems.

Discussion:

See 4.09[1]

- ☐ Other parties' document storage and retention policies.

Discussion:

See 4.09[2]

- ☐ Changes in other parties' software or data storage platforms.

Discussion:

See 4.09[3]

- ☐ Whether other parties use any specialized computer programs peculiar to their specific type of

business.

Discussion:

See 4.09[4]

- ☐ Identity of other parties' key custodians.

Discussion:

See 4.09[4]

- ☐ Consider what data format to request:

- ☐ Native format.
- ☐ TIFF or PDF format with load file.
- ☐ Printed.



134 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 4 Planning E-Discovery

II. DETERMINING USE AND EXTENT OF E-DISCOVERY IN CASE

1-4 MB Practice Guide: CA E-Discovery and Evidence 4.04

AUTHOR: Steve Williams

4.04 Options and Strategies.

Documents and information in electronic form are now a routine part of discovery in civil actions. Discovery planning should begin with the presumption that most forms of discoverable information will be retrieved from computer networks, hard drives, desktop computers, laptop computers, and even devices such as cell phones and Blackberries. These sources of discoverable information may be supplemented with more typical hard copy documents. The prevalence of electronic information requires attorneys to evaluate their discovery needs and planning in new and different ways.

California law, consistent with federal law involving electronic discovery, recognizes the burdens and expense that may be posed by electronic document preservation, retrieval, review, and production and provides procedures for parties to identify these issues, discuss them, and present them to the court when necessary.



Strategic Point:

In some instances the supposed burdens are exaggerated and it will be the job of counsel to disabuse the court of the notion that e-discovery always imposes unreasonable burdens.

Evaluating electronic discovery issues requires an understanding of the parties who are likely to have relevant information and the materials and information systems that those parties use. An attorney must understand and be able to explain to the court the types of hardware, the format of media, and the process by which information is created, maintained, and produced. It is difficult to properly plan for e-discovery without understanding how electronic information is stored and maintained. This is the reason why both California and federal law call for an early meeting of counsel to discuss e-discovery issues, including preservation of ESI, forms in which information will be produced, the timing of productions, the scope of discovery, how issues of privilege will be addressed, how issues of confidentiality, privacy, and trade secrets will be addressed, and how the costs of search and production will be borne [see *Cal Rules Ct, Rule 3.724*]. Understanding basic principles that govern e-discovery permits the proper evaluation of e-discovery issues and the development of an appropriate discovery plan. An attorney must educate himself or herself, the client, other parties, and the court in order to ensure that a discovery plan is in place that will provide for the appropriate review and production of e-discovery.



135 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 4 Planning E-Discovery

II. DETERMINING USE AND EXTENT OF E-DISCOVERY IN CASE

1-4 MB Practice Guide: CA E-Discovery and Evidence 4.05

AUTHOR: Steve Williams

4.05 Counsel Must Assess Need for E-Discovery.

4.05[1] Counsel Must Determine Importance of ESI in Case. Counsel must evaluate at the outset of a case whether ESI relevant to the case may exist and, if so, whether to obtain it using the California state court e-discovery process discussed in this publication. This process should begin at the time the attorney first accepts the case, before litigation is filed.

4.05[2] Nearly Every Case Involves ESI. Some attorneys continue to believe that e-discovery is not an issue in their cases, and that e-discovery issues only exist in complex litigation. This is not so. ESI potentially exists in any case in which a party or witness may have used a computer, cell phone, or Blackberry. Given how ubiquitous these devices are, it is apparent that it will be the rare case in which ESI is not potentially relevant.

Examples:

- In a simple auto accident case, it may be critical to determine whether a driver was using a cell phone or "texting" when an accident took place. The telephone company would have ESI that can answer this question.
- In estate litigation, the contents of a defendant's home computer could be important to demonstrate undue influence (e.g., e-mails to a testator or third parties regarding changes in the testator's estate plan) or the improper use of estate funds by a trustee or other fiduciary.

4.05[3] Counsel Should Not Assume That E-Discovery Is Not Feasible. Moore's Law states that processing power doubles about every 18 months relative to cost or size, and a similar observation (sometimes called Kryder's law) states that storage disk density doubles annually. A result of these "laws" is that ESI is vastly easier and cheaper to create and store, resulting in the proliferation of data we face today.

It is axiomatic that discovery poses challenges to parties in litigation, but in reality, the same technology that led to the mass amount of data at issue continues to make that data usable. The point of this is that advances in technology have

made data mining more feasible, so that the common presumption that ESI is inaccessible due to cost and burden often is not justified.



Warning--Attorneys Should Stay Up to Date on E-Discovery Issues:

A practitioner cannot simply rely on prior experience with e-discovery in determining its use and extent in a particular case. Instead, attorneys must keep up to date on the most advanced and economically feasible means of addressing e-discovery issues in a given case. Available resources abound in publications such as this one, legal newspapers and magazines, and webinars. It is recommended that practitioners update themselves at least twice a year concerning the state of the art.



Cross Reference:

Attorney's duty of competency, see *Ch. 3, Ethical Issues for Attorneys in E-Discovery*, 3.21.



136 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 4 Planning E-Discovery

II. DETERMINING USE AND EXTENT OF E-DISCOVERY IN CASE

1-4 MB Practice Guide: CA E-Discovery and Evidence 4.06

AUTHOR: Steve Williams

4.06 Counsel Must Determine Potential Scope of E-Discovery in Particular Case.

4.06[1] Subject Matter and Location of ESI Should Be Considered. E-discovery changes the means by which discovery takes place, and those changes have profound implications for the scope of discovery. Scope of discovery in this context has two primary meanings:

- The subject matter of discovery, and
- The places where discoverable information is likely to reside.

In the past, discoverable information resided primarily in the hard paper files of percipient witnesses and in the archival hard copy files maintained by a party. Now, discoverable information may reside in a multitude of locations, including:

- Computer networks.
- Servers.
- Desktop computers.
- Laptop computers.
- Cell phones.
- Blackberries.
- Personal data assistants (PDAs).
- Flash drives.

- Memory sticks and cards.
- Printers.

The above list contains only the most common repositories of ESI, and is far from exclusive.



Strategic Point--Negotiated or Court-Imposed Limitations on E-Discovery.

As the law concerning e-discovery has developed, it has become increasingly common that a party responding to discovery will negotiate a single set of search terms to be used and custodians whose documents will be searched. Courts are encouraged to limit the frequency with which searches of electronic information must be performed. As a result, the initial search for and production of documents by a responding party may be the only time that the responding party produces documents in a case. For this reason, it is critical to ensure that the initial search captures all terms and custodians that can be reasonably anticipated at that time. Unless good cause is shown, a court may not permit subsequent searches for documents after an initial search, or may greatly limit the scope of a second or third search for documents [CCP § 2031.280(d)(2) ["[a] party need not produce the same electronically stored information in more than one form"]].

4.06[2] Extent of E-Discovery Will Depend on Nature of Case. Although ESI is relevant in most cases, the *scope* of e-discovery may vary substantially depending on the nature of the case. This simply means that, as in any case, counsel must ascertain what type of e-discovery will be at issue and develop an appropriate discovery plan relative to the expected e-discovery. If only minimal e-discovery is at issue, developing this plan will be straightforward and simple.



Warning:

Even if the e-discovery plan will be simple, it should not, however, be ignored.

Example:

It may be critical to determine whether a driver was using a cell phone or texting when an accident took place. While this may be the only e-discovery issue in the case, it could also be the single most important discovery issue in the case. Because many forms of ESI are periodically deleted or modified, failure to focus on e-discovery issues early in the case could lead to the loss of critical evidence that could have simplified resolution of the case.

4.06[3] Nature of Parties and Witnesses Will Play Major Role in Determining Scope of E-Discovery. The nature of the parties and witnesses will play a large role in determining how e-discovery will be at issue in a case.

Examples:

- A case involving individuals is likely to have a relatively small but still important e-discovery component--for example, home computers and cell phones may be all that is at issue.
- Cases involving any organization of any size--a business, public entity, or nonprofit corporation--will involve much more complexity and will require counsel to make a preliminary assessment of the likely witnesses in the case and the computer networks and servers they use.



137 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 4 Planning E-Discovery

II. DETERMINING USE AND EXTENT OF E-DISCOVERY IN CASE

1-4 MB Practice Guide: CA E-Discovery and Evidence 4.07

AUTHOR: Steve Williams

4.07 Counsel Should Evaluate Advantages and Benefits of E-Discovery.

4.07[1] ESI Can Be Essential to Win Case. The challenges presented by e-discovery can be offset by its advantages. The first and foremost advantage is simply that ESI may be essential to the case, leaving counsel with little choice but to seek discovery of ESI. It can be the most relevant evidence and have the potential to resolve contested issues in the litigation the most quickly. Because the majority of communications and documents are stored today in electronic form, it may simply be impossible to win the case without it.

Example:

In *Covad Communications Co. v. Revonet, Inc.* (DDC 2009) 258 FRD 5, the court noted that metadata of access to database files would allow speedy resolution of the case: "If the forensic imaging shows little use of the data from Covad by Revonet, Covad's financial motivation to continue this lawsuit may disappear or at least lead to an early settlement. If, on the other hand, the data contradicts Revonet's assertions, made throughout the lawsuit, that Revonet made little use of the Covad data, then the shoe will be on the other foot. In either event, the data simply must be found and analyzed before the parties and the Court can get their hands around what this case is truly worth. It is simply one of those perhaps unusual cases where paradoxically 'the amount in controversy,' 'the likely benefit,' and the 'needs of the case' can only be ascertained by permitting the discovery sought. ... Second, while the issues at stake in this commercial controversy may be not be of interest to anyone but these litigants, they still have a right to its speedy and just conclusion, which, in my view, will be advanced by the forensic imaging. I know of no other way to examine the data and how it was used by Revonet." [*Covad Communications Co. v. Revonet, Inc.* (DDC 2009) 258 FRD 5, 12--13. While the *Covad* court suggested that the need for prompt ESI discovery was "unusual," it is expected that focused ESI discovery may lead to prompt resolution of many cases. This is a further reason why a technological understanding, coupled with command of procedure and the facts of the case, may enable parties to resolve cases more quickly and less expensively than was previously the case.

4.07[2] E-Discovery Can Result in More Focused Discovery. E-discovery can result in more focused discovery, including the following:

- A well thought-out search protocol that identifies appropriate search terms and sources of electronic information to be searched can result in a better production of documents that can be accomplished more quickly.
- The core documents in a case are more likely to be identified earlier than previously possible.
- It may be possible to eliminate duplicate documents and to reduce the production of irrelevant documents.
- As a result of the proper negotiation of custodians, search terms, and metadata, the document production will more readily lend itself to use, including use in litigation document management software programs.
- It may be easier to prepare for depositions and trials using searchable, well-organized ESI.

4.07[3] E-Discovery Can Facilitate Better Case Management Planning. A corollary to the enhanced focus on the substance of the case that results from developing an e-discovery plan is the fact that the search for and production of documents is more likely to take place a single time, rather than in a seriatim fashion. Repeated requests for production have a tendency to cause litigation to expand. Sometimes this is justified by unexpected revelations in the course of discovery; more often, repeated requests for production are the result of a lack of focus on appropriate discovery at the outset.

The new realm of e-discovery forces counsel to think more comprehensively earlier in the case. This should lead to more efficient litigation as discovery requests are more likely to be tailored to the actual issues in dispute.



Warning:

A failure to properly focus on discovery issues at the outset could have negative consequences because there is a lesser likelihood that case management orders will be revised during the course of litigation. Instead, courts will expect that parties have properly anticipated the appropriate scope of discovery and will be more likely to require a showing of good cause to extend or modify a case management schedule for discovery purposes.



138 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 4 Planning E-Discovery

II. DETERMINING USE AND EXTENT OF E-DISCOVERY IN CASE

1-4 MB Practice Guide: CA E-Discovery and Evidence 4.08

AUTHOR: Steve Williams

4.08 Attorney Should Evaluate Challenges of E-Discovery.

4.08[1] Attorney May Have to Learn New Technology and Procedures. The first challenge posed by e-discovery is the need to learn the relevant terminology and procedures, with which attorneys often are unfamiliar. Lack of familiarity with terms of art will result in an inability to effectively determine the sources of data that should be subject to discovery, the means by which those sources will be searched for discoverable information, the reasonableness of proposed searches for discoverable information, and the evaluation of whether the costs and burdens of searching sources of electronic information outweigh the benefits of production. For example, few attorneys would prefer to receive terabytes of information if a more focused request would result in a reasonable production. Failure to understand terminology could lead to this unintentional result. Without a proper understanding of these issues, an attorney will not only be at a disadvantage in negotiating proper discovery with his or her adversary but will also be at a disadvantage in explaining to the court why his or her proposals should be accepted rather than those of the adversary.

Example:

The need to understand terminology is demonstrated in *Columbia Pictures Inc. v. Bunnell* (CD Cal 2007) 245 FRD 443 . That decision is commonly understood to be an example of the "unreasonable" burden of ESI, but actually involved a relatively simple procedure to preserve computers' random access memory, which unquestionably held relevant evidence in the case. All that was required to preserve the evidence was for the defendants to enable the logging function of their servers. Without an understanding of random access memory and its role in storing information, an attorney would be unable to brief a court on its importance and explain why it should be preserved. Issues like this abound when it comes to ESI, and technology develops so rapidly that it is essential to keep up to date.

Consider:

A good starting point for practitioners is to review the work of the Sedona Conference on e-discovery. The Sedona Conference has been very influential, particularly in the federal courts. Materials produced and published by the Sedona Conference can be found at www.thesedonaconference.org.

Consider:

Retaining a consultant to assist in ESI issues should also be considered. In *Rhoads Indus. v. Bldg.*

Materials Corp. of Am. (ED Pa 2008) 254 FRD 216, the court held that counsel had acted reasonably in trying to avoid production of privileged materials by retaining an e-discovery consultant who used sophisticated software for searching for privileged e-mails. For discussion of obtaining expert assistance in e-discovery, see 4.11 et seq.

► **Cross Reference:**

Technology and terminology relating to ESI and e-discovery, see Ch. 1, Understanding Electronic Evidence.

4.08[2] E-Discovery Presents Timing Challenges.

4.08[2][a] Counsel Must Develop Working Knowledge of Terminology and ESI Production Prior to "Meet and Confer" Meeting. Counsel must develop a working knowledge of terminology and practices relating to the production and storage of electronic information early in a case so that counsel is prepared for the "meet and confer" meeting of counsel that should take place at an early point.

► **Cross Reference:**

Discussion of "meet and confer" requirement and strategy, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferring, and Case Management Conference*, 5.14-5.25.

4.08[2][b] Counsel Must Identify Key Custodians Early in Process. At an early point in the process, it is necessary to determine who the key witnesses are, so that search protocols are designed that are reasonably likely to retrieve the documents subject to discovery from those custodian's files. This entails identifying the key witnesses, determining where electronic files related to the witnesses are likely to be--e.g., the witnesses' computers, network servers used by the witness, the computers of assistants, secretaries, and associates of the witness, and PDAs used by the witness.

► **Cross Reference:**

Discussion of key custodians, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferring, and Case Management Conference*, 5.06[8], 5.19[2].

4.08[2][c] Counsel Must Decide on Search Methods Early in Process. Search terms and methods must be devised early in the case. The net result of this is that a much more comprehensive understanding of a case must be developed early to ensure effective discovery will be taken.

► **Cross Reference:**

Discussion of search methods, see *Ch. 9, Gathering and Producing Electronically Stored Information*, 9.19-9.28.

4.08[2][d] Use of E-Discovery Can Increase Overall Discovery Time. Because of the large volume of electronically stored information in a typical case, search, review, and production of ESI may require more time than other forms of discovery. While California's discovery rules typically contemplate a 30-day period in which to respond to discovery requests, in cases in which large amounts of ESI are involved it is likely that the parties will need to build in larger periods for document productions and perhaps the use of "rolling productions" (in which ESI is produced in sections as review is completed). For example, it is not uncommon to have hundreds of thousands of e-mails that must be reviewed for relevance and privilege by large teams of reviewers. Such reviews require time for planning, training, coordination and quality control of the review teams. Failure by the parties to discuss the timing of production creates the risk of setting unrealistic time frames for case management which, in turn, will impede the ability of the parties to properly prepare the case for discovery and trial. This is one of the reasons that the "meet and confer" process for

e-discovery [see *Cal Rules Ct., Rule 3.724(8)*] is so important.

 Cross Reference:

Litigation holds and notices to opposing counsel, see *Ch. 5, Initial Procedures in E-Discovery: Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference*, 5.05-5.07, 5.19[2].

4.08[3] Consultants or Experts Are Often Necessary. Because of the amount of technical knowledge that is required to understand and conduct e-discovery, when a case involves e-discovery issues it is essential to acquire the requisite expertise to develop a discovery plan and to negotiate with the parties in the case. An attorney who does not have this knowledge, or access to people with such expertise, should find an appropriate consultant or expert.

 Cross References:

Use of e-discovery experts, see 4.12, 4.13.

E-discovery vendors, see 4.14.

4.08[4] Counsel Must Consider Potential Cost of E-Discovery.

4.08[4][a] E-Discovery Can Be Extremely Expensive. The costs of e-discovery can easily dwarf the costs of productions of paper documents. In large cases, outside vendors typically are necessary to host large productions of documents because the volume of materials produced would tax the resources of most law firms. The costs of production and maintenance of documents is one of the most important things to consider when planning for the cost of discovery in a case, as these may be recurring costs.

Although the respondent ordinarily bears the burden of the cost of actual production of information [see *San Diego Unified Port Dist. v. Douglas E. Barnhart* (2002) 95 CA4th 1400, 1404, 116 CR2d 65], the proponent still must review and evaluate the ESI to determine what is actually relevant and usable in the case. This can take many hours of time, and will have to be done either by the firm's personnel or outside vendors, often at significant cost. If an attorney pursues vast productions of information, the result might be a costly and burdensome effort to root through the avalanche of data for relevant information.

 Warning:

The attorney should consider at the outset whether a request for all potentially relevant ESI is going to be cost effective, and whether limits on what is requested make financial sense in light of the issues and dollar amount at stake in the litigation.

 Warning:

Courts may limit the frequency or extent of ESI discovery in circumstances including where "the likely burden or expense of the proposed discovery outweighs the likely benefit, taking into account the amount in controversy, the resources of the parties, the importance of the issues in the litigation, and the importance of the requested discovery in resolving the issues" [CCP §§ 1985.8(h) (third-party subpoenas may be limited), 2031.060(f), 2031.310(g)].

 Cross Reference:

Budgeting for e-discovery, see 4.17

4.08[4][b] Counsel Must Evaluate Potential for Cost-Shifting to Requesting Party. In addition to the actual expense of reviewing and evaluating ESI, a requesting party may be obligated to pay for the costs of the respondent's

ESI production if the responding party can demonstrate that the burden and expense of production make cost-shifting appropriate--a finding courts are increasingly willing to make [CCP § 2031.060(e)]. A requesting party who insists that inaccessible electronic documents be restored to a format in which they can be reviewed may also be obligated to pay those costs [CCP §§ 2031.280(e), 1985.8(g)].

California law, like federal law, permits courts to order that the cost of searching for and producing electronically stored information be shifted to the requesting party [CCP § 2031.060(e)]. This can also include the cost of restoring inaccessible data to a format in which it can be used. "If necessary, the responding party at the reasonable expense of the demanding party shall, through detection devices, translate any data compilations included in the demand into reasonably usable form" [CCP §§ 2031.280(e), 1985.8(g)].

**Warning:**

These concerns are heightened when third parties are subject to discovery [CCP § 1985.8]. Since third parties frequently have no stake in the litigation, and often merely happen to be in possession of relevant evidence, courts may be even more likely to shift the burden of producing the ESI to the party who wants to obtain it.

**Strategic Point--Cost Shifting Arguments Should Be Formulated Early in Case:**

Because of the potential financial effect of cost shifting and the increased willingness of courts to shift costs to the propounding party, it is critical to consider this issue early in the planning process, tailor the e-discovery plan to the needs of the case, and be able to explain to a court why the proposed discovery should not result in cost-shifting. Conversely, when responding to ESI requests, the responding party should consider whether a response requires "translation" and therefore cost-shifting may be appropriate.

Example:

Toshiba America Electronics Components v. Superior Court (2004) 124 CA4th 762, 21 CR3d 532 predates the California Electronic Discovery Act and rules, but nevertheless provides instruction on how courts are likely to approach such matters because the case involved a statute providing for mandatory cost-shifting for data translation. In *Toshiba*, the court reversed as an abuse of discretion a trial court order that required restoration and translation of data from backup tapes without determining whether the demanding party should pay the cost of translating the data into usable form.

**Cross References:**

Respondent's procedure for seeking cost shifting, see *Ch. 9, Gathering and Producing Electronically Stored Information*, 9.15-9.18, 9.35.



139 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 4 Planning E-Discovery

II. DETERMINING USE AND EXTENT OF E-DISCOVERY IN CASE

1-4 MB Practice Guide: CA E-Discovery and Evidence 4.09

AUTHOR: Steve Williams

4.09 Counsel Should Learn About ESI From Responding Party.

4.09[1] Learning About Responding Party's Electronic Systems Is Essential. Nothing is more important to a discovery plan than understanding the information systems of parties and witnesses. Counsel must develop an understanding of the computers and networks being used; the manner in which information is created, backed up, and stored; and the document retention and destruction policies at issue. Some matters are common to almost all parties, and others may be more specific to specific types of entities.



Timing--Preparation for the "Meet and Confer" Conference:

Counsel must begin learning about ESI issues in a case before the first meet and confer prior to the first case management conference. Counsel should begin by understanding his or her own client's ESI systems and issues. Understanding what ESI issues will be difficult for counsel's own client will allow counsel to try to guide the parties to an agreement that will resolve issues in favor of counsel's client, or alternatively, set the stage to seek a court order resolving the ESI issues favorably for the client.

Counsel must also investigate what ESI the other parties have, and how it will be preserved, gathered, and produced. This investigation may include interviews of counsel's own client, questions at the meet and confer conference, and if necessary, interrogatories or depositions about ESI topics. At the meet and confer for the case management conference, counsel must have a sufficient understanding of the case, the parties, and the anticipated issues relating to e-discovery so that the appropriate questions can be asked and so that proper steps can be taken to follow up and get the information necessary to properly plan for e-discovery. If counsel is not able to understand what the other parties describe and ask questions designed to elicit the necessary information, it will not be possible to adequately prepare for the meeting of counsel or for the first case management conference.

4.09[2] Other Party's Document Storage and Retention Policies Should Be Investigated. In almost all cases, it will be necessary to determine the electronic document storage and retention policies of other parties:

- First, counsel should determine what e-mail platform is used. Microsoft Outlook and Lotus are the

most common e-mail systems.

- Next, it is necessary to determine the scale on which the e-mail system operates and what servers are used to manage the e-mail system. An e-mail system may be organization wide, or may be maintained on particular servers for particular parts of an organization. This knowledge will assist counsel in determining which servers are likely to have been used by the witnesses at issue in the case.

A proper discovery plan should take into account the servers and backup media for the servers that have been identified through this inquiry.

Once counsel has determined what e-mail systems were used and how they were maintained, it is important to learn what the particular policies and practices were for incoming, draft, sent, and deleting e-mails. For example, e-mail systems might have been set up to routinely delete incoming e-mails from servers--understanding this and confirming that routine deletion has been stopped for relevant e-mails should be a high priority.

Through discussions at the meet and confer and later through interrogatories and depositions as necessary, counsel should try to understand both the formal information systems and policies used by the party and the personal practices of custodians who may deviate from those policies.



Strategic Points:

- An important step in discovery planning should be requesting that parties identify and provide their written policies concerning the use of and retention of e-mail and other ESI.
- Counsel needs to ensure that the discovery plan takes into account incoming and outgoing e-mails on networked systems as well as any e-mails that are resident on individual employees' desktop computers, laptop computers, flash drives, and PDAs.
- The discovery plan should extend to home computers, as it is frequent for employees to use work documents on home computers, transferring documents via e-mails, Citrix servers, or flash drives. This is not limited to e-mails. All manners of documents are almost equally accessible no matter where a person is. Word processing, spreadsheet documents, and e-mails may be accessed, edited, and deleted remotely.

4.09[3] Changes in Respondent's Software or Data Storage Platforms Should Be Identified. It is also critical to discuss with a party whether there have been any significant changes in software programs used by a party as well as platforms on which data is stored. (Previous versions of software or platforms are often referred to as "legacy" systems.) For example, during the time period relevant to a case, a party may have transitioned its data storage from one system to a different system. As a result, archival data may no longer be accessible without undertaking steps to restore such data to make it searchable. The costs of restoring such data for the purposes of searches and productions can be expensive and a responding party is likely to refuse to search such materials on the ground that it is not reasonably accessible. To the extent that a propounding party demands that searches of such material be done, cost shifting may be ordered.

In evaluating whether such materials should be searched and whether cost shifting is appropriate, each side will have to understand the reasonable costs of restoring and searching such information. Often, the party resisting the search and production will assert that the cost of doing so will be prohibitive. A requesting party must be able to understand and test such assertions; failure to do so may result in the denial of such discovery, or alternatively the imposition of the costs of restoring such data to a usable format.

4.09[4] Specialized Programs Should Be Addressed. Specific types of computer programs routinely are used in certain industries. Ascertaining the types of information systems used in a particular industry can be done without undue burden. For example, the insurance industry uses programs that are designed to determine the treatment of claims. Many trading businesses routinely record all telephone communications. It is essential that the information policies of the particular entities involved in litigation are understood in order to properly pursue discovery.

4.09[5] Respondent's Key Custodians for the Parties Should Be Identified. Often, a few people will have generated and/or retained most of the relevant ESI. These individuals are often referred to as "key custodians." Counsel should work with the client to identify and interview the client's own "key custodians" and to identify to the extent possible the key custodians of other parties. It is appropriate to request that at the pre-case management conference meet and confer, a party be prepared to address those individuals who should be within the scope of discovery and why. This benefits both parties, as it permits the party seeking discovery to focus its efforts on those custodians from whom discoverable information is likely to be sought and it permits the party responding to discovery to confine searches of documents to those individuals who are most likely to have responsive documents.



140 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 4 Planning E-Discovery

II. DETERMINING USE AND EXTENT OF E-DISCOVERY IN CASE

1-4 MB Practice Guide: CA E-Discovery and Evidence 4.10

AUTHOR: Steve Williams

4.10 Counsel Should Consider What Format to Request.

4.10[1] Native Format. There is ongoing debate today about whether native format of documents should be sought. A native format production can be unwieldy and difficult to process and review. For example, litigation review platforms may not be able to use native format files. Native format files must be stored in a "read-only" format during review in order to preserve their integrity. Another issue is that the reviewer must have the necessary software to open the native file, and understand the software sufficiently to ensure that the review of the file is complete and accurate. Moreover, because native files do not have a Bates number the way an image does, the parties must ensure that a proper chain of custody can be established between a native file and a printout of the file used at a deposition or at trial. For all of these reasons, a practitioner should ascertain whether there is a real need for native format documents to be produced in case before demanding documents in native format.

In some cases, native format will be required. In business and antitrust cases it is often necessary to have access to information in Excel spreadsheets or other native formats so that parties and experts can analyze data. Excel files, in particular, include both data and formulas which are essential for their use. For example, a printout of an Excel sheet may show a calculated value labeled as "Profit," but only examination of the native Excel file will show the formula that was used to calculate that "profit." Production of this type of information in any form other than native format renders it useless for such purposes. Thus, this type of information should always be requested in native format and an early evaluation must be done to determine what type of information should be produced in native format.

Example:

In *L.H. v. Schwarzenegger (CD Cal 2008) 2008 US Dist LEXIS 86829*, a motion to compel was granted because a producing party produced information, including from databases, in Adobe Acrobat's PDF format. In their native format, the documents were searchable and sortable. In PDF format, they were not. This conversion rendered the information unusable and a further production was ordered.



Strategic Point:

Much of this information about what types of ESI are at issue will have to come from the other parties in

the case, which illustrates the importance of the requirement of *Cal Rules Ct, Rule 3.724(8)* that that parties meet and confer to discuss ESI issues.

Cross References:

Information regarding native format, see *Ch. 1, Understanding Electronic Evidence, 1.22[5]*.

Discussion of notice and meet and confer requirements and procedures, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferring, and Case Management Conference, 5.14-5.25*.

Additional discussion of formats for production of information, and drafting and service production demand, see *Ch. 6, Demanding Production of Electronically Stored Information, 6.09-6.13*.

4.10[2] TIFF Format. A very common mode of production of documents is TIFF files with load files. "TIFF" stands for "tagged image file format." TIFF files are an industry standard type of image file, and readily lend themselves to use in litigation data management systems. "Load files" refers to ASCII text files that are loaded into a litigation management database that contains information about the TIFF images, often including searchable text of the original electronic file, and metadata such as the sender and recipient lines of e-mails.

Cross References:

Detailed discussion of TIFF files, see *Ch. 1, Understanding Electronic Evidence, 1.22[5]*.

Additional discussion of formats for production of information, and drafting and service production demand, see *6.09-6.13*.

4.10[3] Metadata. Metadata has been described as "information about a particular data set which describes how, when and by whom it was collected, created, accessed and/or modified and how it is formatted" [*Williams v. Sprint/United Management Co. (D Kan 2005) 230 FRD 640, 646*] . The Sedona Guidelines state that metadata includes "all of the contextual, processing, and use information needed to identify and certify the scope, authenticity, and integrity of active or archival electronic information or records" [The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information and Records in the Electronic Age, Appendix D: Technical Appendix (Sept. 2004)]. Metadata refers to all of the information about and characteristics of a given document other than its plain text, such as creation date, edit date, send date, received date, view dates, forwarding information, reply information, and copy information. Web-based documents may also contain metadata that could reveal information about Internet use.

Metadata is clearly something that is within the scope of discovery under both California and federal law, but it is frequently the subject of orders denying metadata discovery due to the burden. Neither the California rules nor the federal rules explicitly address whether and how metadata should become the subject of discovery. It is thus up to the parties in a given case to decide if metadata should be produced by, for example, specifying in a discovery request that metadata be produced.

Consider:

Note that a request for production in native file format will also require production of the metadata incorporated in those files, but it is nevertheless good practice to specifically call for metadata production to the extent desired.



Strategic Point--Limiting Metadata Requests:

Before requesting metadata, counsel should decide what particular metadata is necessary and why it is

necessary. While almost all electronic files have some form of metadata associated with or incorporated into them, much of this metadata is not relevant to anything in the litigation. It is unlikely that the vast amount of metadata that is produced will ever be reviewed in any way. Even if metadata is relevant, it may be relevant only for a few individuals and/or a few documents, such as instances when it is necessary to know what a particular person did in relation to a particular document and when. Therefore, it is important to consider tailoring requests for metadata to just those individuals, times, and documents for which you believe metadata is important.

Strategic Point--Important Kinds of Metadata:



Metadata can include such important information as the history of Word and WordPerfect documents, e-mails, and formulas in Excel files. For word processing documents, this includes not only the history and changes made to documents during creation and editing, but can also include notes, comments, communications, and the history of who received, viewed, edited, and forwarded documents. In some business disputes and fraud cases, such information can be critical in determining the intent of parties and in explaining the conduct which they engaged in.

Strategic Point--Alteration of Metadata:



Some types of metadata can be inadvertently altered by gathering the ESI and copying it for review and production (e.g., the file saved date). If such types of metadata are important to review in their unaltered state, this should be made clear to the responding party during ESI meet and confer planning sessions and in the discovery requests seeking such metadata. When preservation of this type of metadata is required, an ESI consultant may need to collect the files in a forensically sound matter.



141 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 4 Planning E-Discovery

III. EVALUATING AND OBTAINING EXPERT ASSISTANCE

1-4 MB Practice Guide: CA E-Discovery and Evidence 4.11

AUTHOR: Steve Williams

4.11 CHECKLIST: Evaluating and Obtaining Expert Assistance.

☐ Determine whether expert assistance will be necessary or advisable for any of following tasks:

- ☐ Preservation of information.
- ☐ Means of retrieving information so that it can be produced in litigation.
- ☐ Processes by which a computer network operates and is backed up.
- ☐ Steps necessary to make backup tapes readable.
- ☐ Developing search terms reasonably likely to discover relevant evidence.
- ☐ Evaluating and understanding limitations on accessibility that are asserted by other parties.
- ☐ Developing sampling methodologies that can inform a decision about what discovery will be permitted.
- ☐ Ascertaining appropriate costs for e-discovery.

Discussion:

See 4.12

☐ Determine which of following roles e-discovery experts will play:

- ☐ Educating counsel.
- ☐ Educating client.
- ☐ Educating court.
- ☐ Participating in conferences of counsel regarding e-discovery issues.
- ☐ Assisting counsel in formulating discovery plan.
- ☐ Collecting e-discovery and maintaining chain of custody.
- ☐ Filtering or narrowing the data population.
- ☐ Assisting with privilege review.
- ☐ Forensic data recovery.
- ☐ Hosting and managing production.
- ☐ Special assistance with confidential information, proprietary databases, and unique data.

Discussion:

See 4.13

☐ Choose an outside e-discovery vendor if necessary for any or all of the following services:

- ☐ Assistance in connection with litigation hold.
- ☐ Data identification and collection.
- ☐ Data review and analysis.
- ☐ E-mail and content archiving and management.
- ☐ Enterprise content and records management.
- ☐ Creation and maintenance of litigation support database.

Discussion:

See *4.14*



142 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 4 Planning E-Discovery

III. EVALUATING AND OBTAINING EXPERT ASSISTANCE

1-4 MB Practice Guide: CA E-Discovery and Evidence 4.12

AUTHOR: Steve Williams

4.12 Options and Strategies.

When a case involves e-discovery issues, it is essential to acquire the requisite expertise to develop a discovery plan and to negotiate with the parties in the case. An attorney who does not have this knowledge, or access to people with such expertise, should find a consultant or expert.

Many types of consultants are available to provide litigation support and expertise in e-discovery issues. Some types of consultants can be expensive, and it is not necessary in all cases to have comprehensive outside consultants to assist with all aspects of electronic discovery. Instead, counsel should evaluate the areas in which assistance is necessary and find a reasonably priced consultant who can provide assistance tailored to the needs of the case.

Typical issues on which outside support may be necessary are:

- The preservation of information.
- The means of retrieving the information so that it can be produced in litigation.
- The processes by which a computer network operates and is backed up.
- The steps necessary to make backup tapes readable.
- Developing search terms that are likely to discover relevant evidence, yet exclude irrelevant ESI to reduce the volume of material that must be reviewed.
- Evaluating and understanding limitations on accessibility that are asserted by other parties.
- Developing sampling methodologies that can inform a decision about what discovery will be permitted.
- Ascertaining the appropriate costs for e-discovery.



143 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 4 Planning E-Discovery

III. EVALUATING AND OBTAINING EXPERT ASSISTANCE

1-4 MB Practice Guide: CA E-Discovery and Evidence 4.13

AUTHOR: Steve Williams

4.13 Counsel Should Determine What Role E-Discovery Experts Will Play.

4.13[1] Educating Counsel. E-discovery experts often assist counsel in understanding the technical issues associated with e-discovery. If counsel does not feel confident discussing and negotiating e-discovery issues, he or she should first find someone to assist in this task. Counsel will not be able to effectively handle discovery in the case until he or she has done so.

4.13[2] Educating Client. Clients, as well as attorneys, need assistance in understanding the rights and responsibilities of parties as they relate to e-discovery; clients will need assistance in understanding these matters. While larger organizations may already have in-house e-discovery expertise, smaller organizations usually need assistance in understanding how e-discovery obligations will affect their business and what they need to do to ensure that they do not violate any obligation they may have to maintain, preserve, search for, and produce documents. Most clients will need the assistance of counsel in helping to budget for the costs relating to e-discovery.

Example:

The need to ensure that clients understand and comply with discovery obligations, and the risk to client and counsel should a client fail to do so, are illustrated by *Phoenix Four, Inc. v. Strategic Resources Corp.* (SDNY 2006) 2006 US Dist LEXIS 32211, in which a client and its counsel were sanctioned because the client had failed to preserve ESI and had failed to ascertain if ESI was available; counsel's failure was its reliance on the client's representation and failure to test those representations [see also *Samsung Electronics Co., Ltd. v. Rambus, Inc.* (ED Va 2006) 439 F Supp2d 524; *Wachtel v. Health Net, Inc.* (D NJ 2006) 239 FRD 81].

4.13[3] Educating Court. A consultant can provide important help in explaining discovery proposals to the court in a manner that fairly and accurately describes what is proposed and why it is reasonable. Most courts do not have the time to delve into the particularities of a given party's electronic data systems, and an attorney must be prepared to provide a road map as to how her proposed discovery plan will accomplish her discovery goals in a manner that does not create undue burden or expense to other parties.

Cross Reference:

E-discovery experts as expert witnesses, see *Ch. 15, Admissibility of Electronic Evidence at Trial*, 15.17, 15.34-15.39.

4.13[4] Participating in Conferences of Counsel Regarding E-Discovery Issues. In some instances, counsel may allow a consultant to participate in meetings of counsel concerning e-discovery issues because counsel does not have complete technical command of a client's electronic data system. In this manner, the parties can ensure the most efficient meeting because technical questions can be answered as they arise. The parties may also agree that information technology personnel may speak directly with consultants on issues relating to the manner in which ESI will be searched and produced.

Some courts have entered orders governing ESI procedures that require each party to designate an individual with knowledge to speak on behalf of the party concerning ESI issues. This role is sometimes filled by outside consultants.



Warning:

When a consultant or a client representative participates in meet and confer meetings, counsel must ensure that the consultant or client understands the importance of accurate communication, and the objectives of such communication. For example, casual, untested, and perhaps inaccurate comments about how easily information could be retrieved might be later used against the client in arguments about the accessibility of the information.

4.13[5] Assisting in Formulating Discovery Plan. Once counsel has identified the key custodians and issues in a case, technical expertise should be sought in ensuring that search terms and methodologies are used that will recover the documents that are reasonably subject to discovery in a case. This includes the specific combinations of search terms and rules that are applied as well as the sources of ESI to be searched.

Example:

In *Rhoads Indus. v. Bldg. Materials Corp. of Am.* (ED Pa 2008) 254 FRD 216, the court held that counsel had acted reasonably in trying to avoid production of privileged materials by retaining an e-discovery consultant who used sophisticated software for searching for privileged e-mails.

4.13[6] Collecting E-Discovery and Maintaining Chain of Custody. Many parties use outside vendors to collect ESI and to establish a chain of custody, and courts have ordered that outside vendors be used in cases in which a party demonstrates an inability--or lack of desire--to comply with ESI obligations [see, e.g., *Dodge, Warren & Peters Ins. Services, Inc. v. Riley* (2003) 105 CA4th 1414, 130 CR2d 385 (ordering expert imaging of data)]. Establishing a chain of custody may require showing that the offered evidence is an identical copy, i.e:

- No information has been added or changed;
- A complete copy of the evidence was made;
- The copying process that was used was reliable; and
- All media were secured.



Warning:

Failure to gather and produce information in a reliable manner could lead to bars on its introduction into evidence. While there is a presumption that a printed representation of computer information or a computer program is accurate [*Evid Code* § 1552(a)], if the party opposing introduction of the evidence can demonstrate that a printed representation of computer information or computer program is inaccurate or unreliable, the proponent of the evidence will have to demonstrate by a preponderance of the evidence

that the printed representation is an accurate representation of the computer information or computer program that it purports to represent [see *Evid Code* § 1552(a)].

Cross Reference:

Introducing ESI at trial, see Ch. 15, Admissibility of Electronic Evidence at Trial.

4.13[7] Filtering or Narrowing the Population. Outside vendors can be of particular importance when very large amounts of information are at issue. In such cases it may be impossible or impracticable to review all documents, and thus it becomes necessary to develop a strategy to limit the amount of information that becomes subject to search and production, or to devise means to search through large volumes of data for only the most pertinent materials. This may be based on date ranges, custodians, or more advanced search techniques. This is a topic that has become particularly important in recent years, and many consultants have expertise in this specific field.

4.13[8] Privilege Review. Vendors can be particularly helpful for the purpose of privilege reviews. Given the volume of documents that may be at issue in large cases, the volume of discoverable information could be more than can be reviewed in the time allowed. Through application of search technology, the volume can be deduplicated for a more focused and quicker review.

Warning:

While using such processes to eliminate duplicate documents from the scope of documents to be reviewed may be helpful, it is important that reduction of duplicates be done in a consistent and appropriate manner that does not interfere with the value and integrity of documents. For example, it may be important to demonstrate that an e-mail was received and reviewed by numerous recipients. The fact that the e-mails were produced by one custodian should not be used as a basis to not produce it from other custodians, or at least to indicate in the production all the custodians who had copies of the e-mails. This may be a topic upon which agreement should be reached as part of a meet and confer process.

Cross References:

Privilege issues and privilege reviews, see Ch. 9, *Gathering and Producing Electronically Stored Information*, 9.36-9.46.

"Clawback" rule and inadvertent disclosure of privileged information, see Ch. 3, *Ethical Issues for Attorneys in E-Discovery*, 3.14.

Discussion of meet and confer process, see Ch. 5, *Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference* 5.14-5.25.

4.13[9] Forensic Data Recovery. If ESI is believed to have been lost, or a party fails or refuses to comply with discovery obligations, consultants may be used to devise means of seeking to retrieve data from networks, backup media, or other devices.

Example:

In *Dodge, Warren & Peters Ins. Services, Inc. v. Riley* (2003) 105 CA4th 1414, 130 CR2d 385, an injunction was issued prohibiting the destruction or deletion of ESI by defendants and requiring a court-appointed expert to copy computer hard drives to search for lost or deleted files. The defendants were alleged to have left the plaintiffs' firm to start their own competing firm. The plaintiff was able to demonstrate that prior to defendants' departure, they had taken electronic materials from the plaintiffs' computer systems. Through this demonstration, the plaintiff was able to ensure that appropriate forensic data recovery would be done before evidence was lost.

4.13[10] Hosting and Managing Production. Counsel needs the ability to store and access the ESI in a reliable way that will allow use of the ESI, but not allow the evidence to be inadvertently altered. For smaller matters in which the software, hardware, and staffing available to counsel are sufficient, counsel may elect to maintain copies of the ESI on counsel's computer network. In larger litigation, it has become commonplace that the scope of documents produced exceeds the capabilities of the parties' counsel to host and maintain. Outside vendors are often used to host some or all of the data produced in a case.



Strategic Point--Court-Appointed Third Party:

In some cases, such as the federal litigation involving the destruction of the World Trade Center in New York on September 11, 2001, the court ordered that a third party be appointed to build, maintain, and operate a database of "core discovery." Despite the plaintiffs' objections concerning the cost of such a project, the court deemed it necessary to ensuring that reliable information was available in the litigation.

Vendors typically charge an initial fee to establish and add to a database, a monthly fee to host the data, and fees per user. As documents are produced in these large cases--typically on hard drive or DVD disks--they are added to the database by the outside vendor. Attorneys then access the materials over the Internet, reviewing the documents on computer. The vendor may also offer services such as optical character recognition (OCR), which creates searchable text from files without text such as scanned paper documents, TIFF files, and PDF files without a text layer. The ability to search documents by text within the document is a key feature for managing and reviewing documents.

4.13[11] Confidential Information, Proprietary Databases, and Unique Data. Expert assistance may be necessary due to unique issues in how a party maintains and uses information. Highly confidential and proprietary information systems may be at issue, and it may not be feasible to demand production of the data in any manner other than that in which it is maintained in order to render the data usable. This may be the case when a database is at issue.

Examples:

- In commercial and antitrust cases, a party's sales data and transactional information may be critical, but may not be maintained in a manner that lends itself to wholesale production. In such instances, queries can be developed designed to retrieve the data sought by the parties.
- Data sometimes may be recorded through proprietary and/or obscure hardware and software systems that cannot simply be copied and produced. In such instances, special steps must be taken to ensure that the data that is needed is made available in a form in which it can be used.
- Data may be stored in a manner that can only be read by certain types of obscure hardware that are no longer in use. Examples include surveillance tapes, telephone recordings, websites, and tachnograph records. Such technical roadblocks may lead to denial of discovery requests and unavailability of the evidence if a proper evaluation is not done and used to explain to a court how and why the data should be searched and produced.



144 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 4 Planning E-Discovery

III. EVALUATING AND OBTAINING EXPERT ASSISTANCE

1-4 MB Practice Guide: CA E-Discovery and Evidence 4.14

AUTHOR: Steve Williams

4.14 Choosing an E-Discovery Vendor.

4.14[1] Types of Vendors. There are many different types of e-discovery vendors. With an unlimited budget, counsel could hire outside consultants to manage every aspect of e-discovery. For those with more limited budgets, vendors are available to perform specific tasks. Counsel needs to analyze the e-discovery needs in light of the budget and decide what tasks the e-discovery vendor will be asked to undertake.

The most important issues to evaluate in determining the type of assistance which may be necessary are:

- The claims and defenses in the case.
- The number of witnesses involved.
- The sources of electronic information at issue.
- The volume of electronic information at issue.
- Any unique issues concerning the types of electronic information involved.



Cross Reverence:

Budgeting for e-discovery, see 4.17.

4.14[2] Vendors Can Assist in Connection With Litigation Hold. The need to preserve and maintain electronically stored information is one of the most challenging aspects in discovery [*see Zubulake v. UBS Warburg (SDNY 2004) 217 FRD 309* (recognizing duty to preserve documents that may be subject to discovery once a party reasonably anticipates that litigation is likely to arise); *Cedars-Sinai Medical Center v. Superior Court (1998) 18 C4th 1, 12-13, 74 CR2d 248, 954 P2d 511* (lawyer customarily instructs client to preserve and maintain any potentially relevant evidence); *Cache La Poudre Feeds, LLC v. Land O'Lakes Farmland Feed, LLC (D Colo 2007) 244 FRD 614* (letter expressing hope that dispute could be resolved without litigation was insufficient to require a litigation hold, but

general counsel's steps to ensure that proper litigation hold was in place once litigation had commenced were inadequate because of insufficient direction to employees, failure to verify completeness, and failure to preserve ESI); *see also* *Lombardo v. Broadway Stores* (2002) 2002 Cal App Unpub LEIS 4700 (unpublished decision sanctioning a party for failure to preserve evidence after receipt of letters demanding preservation)].

This duty can create large burdens and significant costs, and most courts are very cognizant of these challenges and will try to ameliorate these difficulties. There are many services and consultants who can assist parties in putting in place systems that will systematically preserve and maintain what needs to be preserved and maintained, without causing the suspension of normal business routines or undue expense.

**Cross Reference:**

Detailed discussion of litigation holds, *see Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference, 5.05-5.07, 5.19[2]*.

4.14[3] Vendors Can Perform Identification and Collection Tasks. Vendors are available to perform the tasks of identifying sources of ESI, including computers, hard drives, networks, servers, and PDAs, and of developing and performing searches to recover relevant and discoverable information from those sources that is then copied to a hard drive. The consultant should have expertise in litigation matters such that they and counsel can ensure that appropriate means are used to ensure that a proper chain of custody can be established for materials retrieved and produced as a result of the identification and collection of ESI.

4.14[4] Vendors Will Perform Review and Analytics. Vendors are available who will perform simple to comprehensive evaluations and reviews of data that is produced. There are many different means available for searching and analyzing ESI, and new methods are developed constantly.

4.14[5] E-Mail and Content Archiving and Management. E-mail is likely to be a focus for all witnesses in a case. The volume of e-mails can be overwhelming, and the ability to intelligently search for and produce e-mails can pose great challenges. Vendors offer services that include data collection, de-duplication processes, and content and e-mail archiving and restoration.

4.14[6] Enterprise Content and Records Management. These vendors take over all aspects of ESI from inception to long-term storage. This is essentially a means of outsourcing data hosting and management. In recent years many companies have found that it can be less expensive and burdensome to outsource these tasks to vendors with knowledge of litigation issues, including preservation, maintenance, and production of documents. This may minimize burdens to employees and organizations and can create cost savings.

4.14[7] Litigation Support Database. In many instances, discovery documents are maintained remotely by a vendor and accessed through Internet connections. This is typically done in cases with large productions that cannot be maintained on a law firm's computer networks, or when access and review of documents is required at multiple law firms and/or other locations. As documents are produced, they are placed on servers which are then accessed by the attorneys and paralegals. Passwords and protocols are provided for access to the database. These types of services typically involve set up fees and recurring monthly costs, as well as fees per user.



145 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 4 Planning E-Discovery
IV. BUDGETING FOR E-DISCOVERY

1-4 MB Practice Guide: CA E-Discovery and Evidence 4.15

AUTHOR: Steve Williams

4.15 CHECKLIST: Budgeting for E-Discovery.

- ☐ Determine parameters of e-discovery in case.

Discussion:

See 4.03-4.10

- ☐ Determine rates charged by all parties who will participate in e-discovery, including:

- ☐ Attorneys and law office staff.
- ☐ In-house experts.
- ☐ Outside e-discovery vendors.

- ☐ Establish basic expense categories for budget:

- ☐ For party responding to discovery:
 - ☐ Preservation [see 4.17[2].
 - ☐ Collection [see 4.17[3].
 - ☐ Processing [see 4.17[4].

☐ Review [see 4.17[5].

☐ Production [see 4.17[6].

☐ Privilege log [see 4.17[7].

☐ For party requesting discovery, consider cost of:

☐ Analyzing the respondent's ESI sources.

☐ Deciding what to ask for and formulating the discovery request.

☐ Reviewing and analyzing data.

☐ Forensic examination of respondent's hardware and software, if necessary.

☐ Expert testimony and court appearances.

☐ Possible payment of a portion of respondent's discovery costs if negotiated by parties or ordered by court.

Discussion:

See 4.08[4][b] (cost shifting)

☐ Estimate amount of time and expense required for each category of expense.

Discussion:

See 4.17[1]-[8]

☐ Seek ways to keep e-discovery costs manageable, including:

☐ Consider whether costs of particular components of e-discovery plan would outweigh benefits.

Discussion:

See 4.18[1]

☐ Engage in early and ongoing negotiations with opposing party to limit non-essential e-discovery and reduce e-discovery costs.

Discussion:

See 4.18[2]



146 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 4 Planning E-Discovery
IV. BUDGETING FOR E-DISCOVERY

1-4 MB Practice Guide: CA E-Discovery and Evidence 4.16

AUTHOR: Steve Williams

4.16 Options and Strategies.

It is important to prepare a preliminary discovery budget that takes into account e-discovery issues. Failure to do so can lead to rude surprises and disruption. E-discovery can be expensive, and it is important to clients and for management of a law practice that the costs of e-discovery are properly anticipated and provided for. While certainty may not be possible, it should be feasible to prepare a general budget that will permit counsel and client to go forward with eyes open and to ensure that the amount of costs do not become unreasonable in light of the value of the case.



Strategic Point--Budgeting Is Ongoing Process:

Although an attempt to assess the costs of discovery and form a budget for those costs should occur at a very early point in the proceedings, it should be treated as an ongoing process. The scope of discovery is likely to be defined as part of the "meet and confer" process or through other more informal negotiation with the opposing counsel [see 4.09; for discussion of the "meet and confer" process, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferring, and Case Management Conference 5.14-5.25*].

Consider:

Expert and consultant fees usually will be a significant portion of the total budget. They will be essential to explain fundamental issues, ascertaining and ensuring client compliance with e-discovery obligations, developing a plan for e-discovery of other parties and witnesses, and explaining positions on e-discovery to the court. These tasks may continue throughout litigation.



147 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 4 Planning E-Discovery
IV. BUDGETING FOR E-DISCOVERY

1-4 MB Practice Guide: CA E-Discovery and Evidence 4.17

AUTHOR: Steve Williams

4.17 Elements of an E-Discovery Budget.

4.17[1] Summary of Principal Budget Components. The first step in budgeting is to identify the principal categories of cost that are likely to be incurred. The principal elements of an e-discovery budget for *responding to discovery requests and producing documents* are:

- Preservation [see 4.17[2].
- Collection [see 4.17[3].
- Processing [see 4.17[4].
- Review [see 4.17[5].
- Production [see 4.17[6].
- Privilege log [see 4.17[7].

Compare:

The formulation of a requesting party's e-discovery program is similar to that illustrated here, but the categories and relative expense are likely to be different. Although the respondent ordinarily pays discovery expenses, the requesting party nevertheless can expect to incur analysis costs. The following basic categories should be considered:

- Analyzing the respondent's ESI sources.
- Deciding what to ask for and formulating the discovery request.
- Reviewing and analyzing data.

- Forensic examination of respondent's hardware and software, if necessary.
- Expert testimony and court appearances.
- Payment of a portion of respondent's discovery costs if negotiated by parties or ordered by court.

**Warning:**

The respondent's potential e-discovery costs should be a concern to the party seeking discovery, not just to the respondent. The potential for cost-shifting [see *CCP* § 2031.060(b); see also 4.08[4][b]] means that the party seeking discovery will have to take into account the respondent's probable expense and consider whether or not the party seeking the discovery may have to bear a portion of the cost, and what that cost will be [see 4.08].

4.17[2] Preservation. Preservation involves suspending ongoing processes and taking affirmative steps to the extent necessary to ensure that discoverable information is maintained. This may also include the costs to the client of additional backup storage media and other expenses relating to changes in ordinary preservation processes. The cost of preservation will be a smaller component of the budget.

Example:

For purposes of illustration, in a hypothetical case involving a medium size responding party with approximately 40 custodians, the cost of taking appropriate steps to preserve documents might be \$7,500 or less.

4.17[3] Collection. Collection refers only to the process of gathering the documents so that further work can be done. It does not involve processing documents for search and production purposes. As a result, the collection costs will be relatively minor in comparison to other parts of the budget.

At a minimum, a party to litigation will need to collect and gather ESI for production. Sources may include computers, voicemails, and every other means of recording information. Because this must be done in a manner that is reasonably likely to gather material subject to discovery and that preserves the integrity of the ESI being produced, it is essential that this task be performed by someone with the technical expertise to retrieve all appropriate information subject to discovery. The cost of this will depend upon the amount of data and devices at issue.

Collection costs can typically be measured by determining the number of custodians and the volume of data that each custodian has. The initial step is determining the key custodians from whom documents will be searched. In addition to the primary witnesses in the case, support staff for those witnesses should be identified as custodians. Once identified, a reasonable estimate of the amount of data the custodians will have can usually be performed.

Example:

Continuing with the illustrative example in 4.17[1], and assuming a total of 120 gigabytes of information and 8.5 million pages, the cost of collection could be approximately \$10,000.

**Strategic Point--Sampling Can Help Reduce Collection and Review Costs:**

Because of the broad scope of e-discovery, it is sometimes advisable to engage in sampling of a party's electronically stored information. Sampling permits a party to ascertain the likelihood that responsive information will be retrieved from various sources as well as the costs of retrieving such information and the burdens of such production. Sampling also permits a party to test contemplated search protocols to

determine whether they are worthwhile. In both cases, review for both responsiveness and privilege is made much easier. The results of sampling may be used for the purpose of modifying search terms, choosing different or fewer custodians, or choosing to forego entire aspects of a proposed search. The budget for sampling should be relatively modest in light of its purpose of narrowing the scope of discovery.

4.17[4] Processing. Processing involves de-duplicating, applying search terms, and loading the documents into servers for use in the litigation. This process generally refers to the steps taken to identify potentially responsive documents within the entire universe that has been retrieved through the collection process, and eliminating pure duplicates of documents when the production of such duplicates is not essential to the integrity and responsiveness of the document production. These costs are a larger part of the budget than preservation and collection.

Example:

For processing roughly 2.5 million pages of documents, processing fees of approximately \$110,000 may be expected.



Strategic Point--Document Conversions and Allocation of Costs:

When documents are prepared for review, a common approach is to convert the documents into TIFF images, and associate those TIFF images with metadata including searchable text (searchable text will often be created from an electronic document's original content, or through OCR if the electronic document was an image). At present, prices for production of TIFF images and OCR are approximately .035 cents per page of material. The actual expense to each party depends on what, if any, cost sharing arrangements are worked out. It is common for this cost to either be shared by the parties or shifted to the requesting party. In other cases, each side bears the cost of their own processing, but the parties agree to share searchable data.

Alternative platforms may be available to allow native file review or which otherwise do not require TIFFing of images before production, if then.

For large productions with searchable text, computer searches can be used to focus review on pertinent issues. In the case of audio files, services exist to analyze the data and identify responsive recordings by the phonemes used in them.



Cross Reference:

Document processing to facilitate review, see *Ch. 9, Gathering and Producing Electronically Stored Information*, 9.28-9.35, 9.47-9.56.

4.17[5] Review. Review involves application of both electronic searches and manual review to determine responsiveness and to identify potentially privileged documents for further review and preparation of a privilege log. This process may also include identifying and designating documents as confidential in accordance with the terms of a protective order.

Review will likely be the greatest component of the budget by far. The components of this review include staffing the process with attorneys and paralegals to perform the review through a combination of electronic searches and page-by-page review. The review process also requires more senior attorneys to supervise and perform quality control to ensure that the search is being properly performed to retrieve responsive documents while not including non-responsive documents and that potentially privileged documents are being segregated for further review. Estimates of the number of staff needed for the review based upon the number of documents involved, the number of pages per document, and the time in which completion is desired should be made. These estimates should be based upon the

expected production of each level of the review--paralegals, attorneys, and senior attorneys. Applying these staff members' hourly rates to the calculation of expected hours for review, an estimate can be made of the cost of review.

Estimating the cost of such a review can depend upon numerous variables including the type of case at issue, the type of records at issue, the nature of the issues for which review is being performed, the extent to which the documents include privileged or potentially privileged documents, and the application of a single or multiple levels of confidentiality designations.

Example:

A reasonable estimate for a review of approximately 2.5 million pages based upon an average rate of \$225 per hour for paralegal and attorney review, and \$375 per hour for senior attorney review, is approximately \$1,100,000.

Strategic Point--Review Hosting:



Vendors who host document productions typically charge a monthly fee based upon the volume of data and amount of server space being used and the amount of users. Thought should be given for the total amount that will be required to pay the vendor for the service of hosting and providing remote access to documents, as well as when it will be feasible to have adequately reviewed the production such that the amount of documents being hosted can be reduced or eliminated, and the key documents made accessible through more economical means.

Strategic Point--Reduction of Recurring Costs:



There will come a point when the large and recurring costs of e-discovery can be reduced because documents have been reviewed and key documents identified and segregated. Counsel should plan ahead to ramp down recurring costs at the earliest practicable point.

Strategic Point--Seek Ways to Minimize Expense of Attorney Review Time:



As is the case in all forms of discovery, the cost of attorney time for review will be one of the largest components of an e-discovery budget. A paradox to productions of electronic information is that a poorly designed electronic interface for document review or poorly trained reviewers can make it more time consuming to review documents on computer screens than in paper form. This has led some attorneys to have electronic productions "blown back" to paper to enhance the ability to review documents more quickly. However, printing copies of documents for review imposes a per page printing cost that may be very expensive for a large-volume production. Additionally, there may be added costs to dealing with the paper after review to correlate review decisions to the original ESI.

4.17[6] Production. Production refers to the cost of copying the production materials to a media for use by other parties. Production costs often are approximately 10 cents per page.

Example:

The cost of production will be a relatively smaller part of the cost of the overall production process. Based upon a production of approximately 1 million pages at the cost of .10 per page, the cost of production will be approximately \$100,000.00.

4.17[7] Privilege Log. "Privilege log" refers to the more detailed work that must be done to evaluate whether documents that have been identified as potentially privileged are in fact subject to such protection, and the preparation

and service of a privilege log setting forth the essential elements to support a claim of privilege. This step may also include steps taken to maintain privileged documents in a manner separate from non-privileged documents, as well as doing a further review of the produced documents based upon the documents determined to be privileged to ensure that documents have not been produced that are subject to a claim of privilege. Ideally, the review process will have been designed so that reviewers who determine a document is privileged will simultaneously fill out the description and reasons for assertion of privilege in fields for the log.

The work done to prepare a privilege log will need to be done by attorneys taking the appropriate amount of time to review and evaluate the documents. This process can be time consuming because of the care that must go into it to minimize the chances of an inadvertent production and ensure that privileged documents are described with sufficient particularity to prepare an appropriate privilege log.

Based on the number of documents identified as potentially privileged during the review process and the hourly rates of the attorneys performing the privilege log review, an estimate of the costs of this part of the process can be made.

Example:

Assuming a review of approximately 80,000 potentially privileged pages and an hourly rate of \$275 per hour, the cost of preparation of an appropriate privilege log can be roughly \$145,000.



Cross Reference:

Creation of privilege logs, see *Ch. 9, Gathering and Producing Electronically Stored Information*, 9.36-9.46.

4.17[8] Example of Total Budget. To summarize, based on the examples used in the preceding discussion, the total cost of a hypothetical search for and production of documents based on an assumption of 40 custodians and 8.5 million pages of documents, from preservation through production and preparation of a privilege log, is \$1,472,500.00, broken down as follows:

● Preservation \$7,500	[40 custodians]
● Collection \$10,000	[120 gigabytes of information; 8.5 million pages]
● Processing \$110,000	[2.5 million pages]
● Review \$1,100,000	[2.5 million pages @ \$225/hr. for paralegal/attorney review; and \$375/hr. for senior attorney review]
● Production \$100,000	[1 million pages \$.10 per page]
● Privilege log \$145,000	[800,000 pages @ \$275/hour review time]



148 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 4 Planning E-Discovery
IV. BUDGETING FOR E-DISCOVERY

1-4 MB Practice Guide: CA E-Discovery and Evidence 4.18

AUTHOR: Steve Williams

4.18 Counsel Should Seek Limiting Discovery to Save Avoidable Expense.

4.18[1] Counsel Should Consider Whether Costs Outweigh Benefits. Throughout the process of budgeting for e-discovery, counsel for the party seeking e-discovery should consider whether or not the costs of each component of e-discovery sought outweighs the benefits.



Warning--Cost Shifting Affects All Parties:

CCP § 2031.060(a) permits a party from whom electronically stored information is being sought to move for a protective order; one of the bases upon which such a motion may be made is that electronically stored information is "not reasonably accessible" [*see CCP § 2031.060(c)*]. If a responding party has demonstrated that electronically stored information is not reasonably accessible, production of the electronically stored information may still be required if the requesting party shows cause, such as the likely benefit of the requested discovery in relation to the amount in controversy, the resources of the parties, the importance of the issues, and the importance of the requested discovery in resolving the issues [*see CCP § 2031.060(f)*]. A condition of ordering production, however, may be an allocation of the expense of discovery--meaning cost shifting to the party seeking discovery. For this reason, counsel must be careful in what is sought as the expense may outweigh the benefits.



Cross Reference:

Protective orders, see *Ch 3, 3.15*.

Additional discussion of cost shifting, see *4.08*.

4.18[2] Early Negotiations Can Limit Scope and Cost of E-Discovery. Negotiations of e-discovery searches and production have extraordinary importance under the Electronic Discovery Act because the universe of information that will be retrieved will be defined by the scope of negotiations, and because it is unlikely that there will be further searches of electronically stored information. To the extent that subsequent searches are performed, their scope will be limited.

The parties must meet and confer at least 30 days prior to the initial case management conference to address e-discovery issues and how the parties intend to handle those issues [*Cal Rules Ct, Rule 3.724(8)*]. It is anticipated that this "meet and confer" process will provide an opportunity for counsel to meet and decide whether or not limitations on the methods and extent of e-discovery would be beneficial to avoid unnecessary expense to all concerned.



Strategic Point--Send Preservation Letter Before Initiating Negotiations.

One of the first steps that should be done in relation to e-discovery is service of a preservation letter. Unless the court orders another time period, the parties must meet and confer at least 30 days prior to the initial case management conference to address e-discovery issues [*Cal Rules Ct, Rule 3.724(8)*]. It is likely that a court will require a party to preserve and produce documents after receipt of a letter advising the party of the pending or anticipated litigation, of the nature of claims involved, and of the need to preserve and maintain relevant documents [*see, e.g., Lombardo v. Broadway Stores* (2002) 2002 Cal App Unpub LEXIS 4700, 1-2 (imposing sanctions for failure to preserve and produce documents after receipt of preservation demands)]. Service of notice is a means of accomplishing this.



Cross References:

Detailed discussion of preservation letters, and form for preservation letter, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferring, and Case Management Conference*, 5.09-5.13.

Detailed discussion of meet and confer requirement and strategies, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferring, and Case Management Conference*, 5.14-5.25.



149 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.syn

AUTHOR: Ernst Halperin, Practice Consultant

§ 5.syn Synopsis to Chapter 5: Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

5.01 Scope.

5.02 Objective and Strategy.

5.03 CHECKLIST: Preserving Client's Own Electronically Stored Information.

5.04 Options and Strategy for Preserving Electronically Stored Information.

5.05 Consider Duty to Preserve Electronically Stored Information.

5.05[1] General Duty to Preserve Evidence Exists.

5.05[2] Electronic Discovery Act Provides Limited "Safe Harbor" From Spoliation Claims.

5.05[3] Parties Still Have Duty to Preserve Potentially Relevant Information Once Litigation Is Reasonably Likely.

5.05[4] When Duty to Preserve Arises.

5.06 Counsel Should Develop Plan for Preservation of Client's ESI.

5.06[1] Counsel Should Consider Whether Engaging an ESI Consultant Would Be Appropriate.

5.06[2] Data Retention Policy Is a Good Introduction to Client's Systems.

5.06[3] Network Diagrams Help Counsel Understand Client's Data Environments.

5.06[4] Counsel Should Meet With Client's In-House Counsel, IT Personnel, and ESI Consultant to Understand

Client's Data Systems, ESI Retention Practices, and Backup Technology.

5.06[5] Preserving Individual Custodians' Active Data From Routine Destruction.

5.06[6] Developing and Implementing Plan for Preserving Data From Structured Data Systems.

5.06[7] Dealing With Archived Data.

5.06[7][a] Organizations Generally Rotate Disaster Recovery Backup Media on Periodic Basis.

5.06[7][b] Federal Case Law Provides Guidance on Dealing With Archival Media.

5.06[7][c] Taking a Complete Set of Backup Media Out of Reuse Cycle Is Generally Prohibitively Expensive.

5.06[7][d] Proper Understanding of Client's Disaster Recovery Backup Systems Allows Targeted Removal of Media From Reuse Cycle.

5.06[8] Developing and Implementing Plan for Preservation of ESI Located off Client's Network.

5.06[8][a] Individual Custodians Often Have Important Data Stored off Network Servers.

5.06[8][b] Copying ESI Stored on Home Computers of Key Custodians May Be Warranted.

5.06[8][c] Arranging to Copy Custodians' Off-Network Media.

5.06[9] Counsel and Client Should Develop and Implement Plan for Preservation of ESI Located on Legacy Software Systems.

5.06[10] Counsel Should Decide Whether Imaging of Hard Drives May Be Necessary.

5.07 Advising Client of Duty to Preserve.

5.07[1] Disseminating Document Preservation Memos.

5.07[2] Counsel Should Disseminate Periodic Document Preservation Reminders.

5.07[3] Litigation Hold Software Can Be Used in Larger Organizations.

5.07[4] Counsel Should Confer With Document Custodians Periodically to Confirm That Documents Are Being Preserved.

5.07[5] Consider Whether to Inform Opposing Counsel About Preservation Efforts in Order to Head Off Later Assertion That Measures Were Inadequate.

5.08 Consequences of Failure to Preserve.

5.08[1] Counsel Should Beware of Consequences of Failure to Preserve.

5.08[1][a] Sanctions for Spoliation of Evidence May Result.

- 5.08[1][b] Severity of Sanction Is Determined by Culpability and Degree of Prejudice.
- 5.08[2] Opposing Party May Seek Injunction to Protect Against Destruction of Electronic Evidence.
- 5.08[3] Counsel Should Review Possible Consequences With Client.
- 5.09 CHECKLIST: Notifying Opposing Party That E-Discovery Will Be Sought.
- 5.10 Options and Strategy for Notifying Opposing Party.
- 5.11 Preservation Demand Initiates E-Discovery.
- 5.12 Counsel Must Prepare Preservation Demand.
- 5.13 Counsel Must Send Preservation Demand to Opposing Party.
- 5.14 CHECKLIST: Meeting and Confering Regarding E-Discovery
- 5.15 Options and Strategy for Complying With Meet and Confer Requirement.
- 5.16 All Parties Must Meet and Confer to Discuss Specified Issues.
- 5.17 Counsel Must Decide Time, Manner, and Location for Meet and Confer.
- 5.17[1] Meet and Confer Must Occur No Later Than 30 Days Before Date Set for Initial Case Management Conference.
- 5.17[2] Meet and Confer May Be in Person or by Telephone.
- 5.17[3] ESI Meet and Confer May Be Separate or Combined With Meet and Confer to Discuss Non-ESI Issues.
- 5.18 Counsel Must Prepare for Meet and Confer Regarding ESI.
- 5.18[1] Careful Preparation Is Essential.
- 5.18[2] Technical Personnel Should Educate Counsel of Technical Issues.
- 5.18[3] Responding Parties Should Analyze Document Request If One Has Been Served.
- 5.18[4] Counsel's Team Should Identify Issues That Are Likely to Need Resolution.
- 5.19 Parties Should Discuss Particular Issues at Conference.
- 5.19[1] Issues Specified in Rule of Court Must Be Considered.
- 5.19[2] Preservation of Discoverable Electronically Stored Information.
- 5.19[2][a] Counsel Should Inquire About Opposing Party's ESI Creation, Storage, Collection and Document Retention Program.
- 5.19[2][b] Counsel Should Find Out Whether Opposing Party Has Suspended Records Destruction Routine or Imposed Selective Litigation Hold.

5.19[3] Form in Which Information Will Be Produced.

5.19[3][a] Parties Should Address Their Rights and Duties Concerning Form of Production.

5.19[3][b] Hard Copy Production of Electronically Stored Information Is Disfavored.

5.19[3][c] Production in TIFF or PDF With Load Files Is Common.

5.19[3][d] Parties Should Establish Guidelines for Form of Production.

5.19[4] Parties Should Establish Time Within Which Information Will Be Produced.

5.19[5] Parties Should Attempt to Limit Scope of Discovery of ESI.

5.19[6] Counsel Should Discuss Method for Asserting or Preserving Claims of Privilege or Attorney Work Product.

5.19[7] Counsel Should Discuss Stipulated Protective Order for Asserting or Preserving Confidentiality, Privacy, Trade Secrets, or Proprietary Status of Information Relating to Non-Parties.

5.19[8] Counsel Should Discuss How Cost of Production Will Be Allocated Among Parties.

5.19[9] Counsel Should Adopt and Document Proposed Discovery Plan.

5.19[10] If Opposing Counsel Is Not Forthcoming, Counsel Should Consider Propounding Interrogatories or Noticing a Deposition.

5.20 Counsel Should Identify Areas of Agreement and Disagreement.

5.20[1] Counsel Should Determine Which Issues Parties Can Agree On.

5.20[2] Counsel Should Consider Whether Court Intervention May Be Necessary for Unresolved Issues.

5.21 Counsel Should Prepare and Execute Any Formal Agreements Negotiated at Conference.

5.22 CHECKLIST: Attending Case Management Conference.

5.23 Options and Strategy Regarding E-Discovery Issues at Case Management Conference.

5.24 Counsel Must Attend Initial Case Management Conference.

5.24[1] Court Must Set Initial Case Management Conference.

5.24[2] Meet and Confer Identifies Issues for Case Management Conference.

5.24[3] Counsel Must Attend Initial Case Management Conference If Required.

5.25 Counsel Must Determine What Orders Should Be Entered Relating to Discovery of Electronically Stored Information.

5.25[1] Court Must Enter Case Management Order.

5.25[2] Any Agreements Reached by Parties at Meet and Confer Should Be Incorporated Into Case Management and Other Orders.

5.26 Sample Document Preservation Memorandum (Litigation Hold).

5.27 Client ESI Interview Checklist.

5.28 Demand Letter with Document Preservation Demand.

5.29 Interrogatories Regarding Electronically Stored Information.

5.30 "Meet and Confer" Checklist.

5.31 Sample ESI Production Protocol.

5.32 Sample Letter to Opposing Counsel Regarding Document Preservation Steps Taken.

Ernst Halperin, Practice Consultant n*

FOOTNOTES:

(n9)Footnote *. Law Office of Ernst Halperin, San Francisco. Previously a partner with the San Francisco firm of Folger Levin & Kahn LLP, Mr. Halperin has litigated complex commercial, bankruptcy, and intellectual property cases since 1995. He has managed the discovery of ESI in cases alleging breach of merger agreements, trade secret misappropriation, fraudulent transfers, construction defects, and patent infringement. He currently practices as a dispute resolution neutral.



150 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference
I. STRATEGY

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.01

AUTHOR: Ernst Halperin, Practice Consultant

5.01 Scope.

This chapter covers:

- Objectives and strategy for initial procedures in e-discovery [see 5.02].
- Duty to preserve electronically stored information [see 5.05].
- Developing a plan for preserving ESI from routine destruction [see 5.06].
- Advising clients of the need for preservation, and consequences of failure to preserve [see 5.07-5.08; Forms 5.26, 4.17].
- Notifying opposing party that e-discovery will be sought [see 5.10-5.13; Form 5.28].
- Prepare for e-discovery conference [see 5.16].
- Topics to discuss with opposing counsel at the e-discovery conference [see 5.18-5.19].
- Attending conference [see 5.20].
- Discussing e-discovery issues at the case management conference [see 5.23-5.25].
- Interrogatories for use in gathering information about the opposing party's electronically stored information [see Form 5.29].

Core Statutes:

Cal Rules Ct, Rule 3.724



151 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference
I. STRATEGY

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.02

AUTHOR: Ernst Halperin, Practice Consultant

5.02 Objective and Strategy.

Initial procedures in e-discovery involve identifying and preserving relevant electronically stored information. Because e-discovery is a two-way process, counsel first should meet with his or her own client's IT personnel to develop a defensible plan for complying with the client's own evidence preservation obligations.

Counsel then should send the opposing party a notice that ESI will be sought, along with a preservation demand, both to remind the opposing party of its preservation duty, and to lay the groundwork for sanctions in the event that the opposing party does not preserve ESI important to the litigation.

All parties are required to meet and confer no later than 30 days before the date set for the initial case management conference to consider issues relating to the discovery of electronically stored information. The parties are encouraged to develop a proposed plan relating to e-discovery, to avoid subsequent disputes, protect privilege and privacy concerns, and keep discovery costs manageable [see *Cal Rules Ct, Rule 3.724(8)*].

If the opposing party is not forthcoming about its electronically stored information, consider using interrogatories and/or deposition notices to determine what information exists, the opposing party's operating system, access to backup tapes, and any document retention and disposition policy.



152 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

II. PRESERVING CLIENT'S OWN ELECTRONICALLY STORED INFORMATION

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.03

AUTHOR: Ernst Halperin, Practice Consultant

5.03 CHECKLIST: Preserving Client's Own Electronically Stored Information.

☐ Understand when duty to preserve evidence arises:

Discussion:

See 5.05, 5.06

☐ Preservation duty attaches to any information a party reasonably knows is:

☐ Relevant to action or potential action.

☐ Has been or is likely to be requested during discovery.

Discussion:

See 5.05[1]

☐ Electronic Discovery Act provides a limited "safe harbor" from spoliation claims for routine, good-faith operation of an electronic information system.

Discussion:

See 5.05[2]

☐ Parties still have duty to preserve potentially relevant information once litigation is reasonably likely.

Authority:

5.05[2]

Discussion:

See 5.05[3]

- ☐ Duty to preserve arises when party has notice that the evidence is relevant to litigation or when a party should have known that evidence may be relevant to future litigation.

Discussion:

See 5.05[4]

- ☐ Develop plan for preservation of client's ESI in consultation with a project team made up of in-house counsel, client's IT personnel, and, if appropriate, ESI consultant.

Discussion:

See 5.06

Form:

See 5.27

- ☐ Consider engaging an ESI consultant.

Discussion:

See 5.06[1]

- ☐ Review client's data retention policy.

Discussion:

See 5.06[2]

- ☐ Review client's network diagram.

Discussion:

See 5.06[3]

- ☐ Meet with in-house counsel, IT personnel, and ESI consultant to understand client's information technology environment.

Discussion:

See 5.06[4]

- ☐ Develop plan for preserving individual custodians' active data.

Discussion:

See 5.06[5]

- ☐ Develop plan for preserving data from structured data systems.

Discussion:*See 5.06[6]*

- ☐ Develop plan for preserving archived data.

Discussion:*See 5.06[7]*

- ☐ Develop plan for preserving ESI located off client's network.

Discussion:*See 5.06[8]*

- ☐ Develop plan for preserving ESI located on legacy software systems.

Discussion:*See 5.06[9]*

- ☐ Disseminate document preservation memorandum, reminders to preserve evidence, and confer periodically with document custodians to confirm compliance.

Discussion:*See 5.07***Form:***See 5.26*

- ☐ Determine whether there are grounds for an injunction to protect against opposing party's destruction of electronic evidence.

Discussion:*See 5.07[2]*



153 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

II. PRESERVING CLIENT'S OWN ELECTRONICALLY STORED INFORMATION

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.04

AUTHOR: Ernst Halperin, Practice Consultant

5.04 Options and Strategy for Preserving Electronically Stored Information.

The first step in the e-discovery process is document preservation to ensure that discoverable evidence is not lost through the routine operation of computer systems, or through willful destruction. Counsel should deal with his or her own client first, learning about the client's organization and electronic information systems, and understanding the client's ESI retention policy and actual practices.

Counsel should work with the client's information technology personnel to develop a plan to preserve ESI from routine destruction. Counsel should also work with the client to disseminate a document preservation memorandum to custodians of ESI, explaining the duty to save relevant information, describing what types of information need to be preserved, and the consequences of the failure to preserve. Counsel should meet with the client and develop the procedures for preserving ESI as soon as practicable after it becomes apparent that litigation is imminent. In some instances this will mean meeting with the client after a summons and complaint has been served on the client. However, in other instances, this meeting should occur even before litigation has commenced. The duty to preserve evidence arises when a party reasonably should know that evidence exists that may be relevant to the subject matter of an anticipated lawsuit.

Some attorneys plan for e-discovery before litigation is even on the horizon by working with their clients' information technology personnel to establish data segregation systems that are intended for litigation rather than relying on the existing systems designed for data recovery [see Loomis, *Barristers Tips: Creating Effective Electronically Stored Information Systems*, 32 *Los Angeles Lawyer* 8 (November, 2009); see also Ch.16, *Establishing Best Practices Regarding Electronically Stored Information*].

Counsel may also demand that the opposing party preserve relevant evidence. Such a request should identify the issues in the lawsuit, the types of documents likely to be requested during discovery, and the time period relevant to the lawsuit. If there is reason to believe that the opposing party may be engaging in the willful destruction of electronically stored information, counsel should consider obtaining an injunction to protect against that destruction.



154 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

II. PRESERVING CLIENT'S OWN ELECTRONICALLY STORED INFORMATION

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.05

AUTHOR: Ernst Halperin, Practice Consultant

5.05 Consider Duty to Preserve Electronically Stored Information.

5.05[1] General Duty to Preserve Evidence Exists. A party, or anyone who anticipates being a party, to a lawsuit has a duty to not destroy evidence [*Cedars-Sinai Med. Ctr. v. Superior Court* (1998) 18 C4th 1, 874 CR2d 248, 954 P2d 511] . A litigant "is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request" [*Zubulake v. UBS Warburg LLC* (SDNY Oct 2003) 220 FRD 212, 217] .

► Cross Reference:

Discussion of preservation duties and document retention and deletion policies, see Ch. 16, Establishing Best Practices Regarding Electronically Stored Information.

5.05[2] Electronic Discovery Act Provides Limited "Safe Harbor" From Spoliation Claims. The Electronic Discovery Act recognizes that the routine, good faith operation of an organization's electronic information systems may destroy or alter ESI, and the statute provides a limited "safe harbor" from sanctions that would otherwise result. "Absent exceptional circumstances, the court shall not impose sanctions on a party or any attorney of a party for failure to provide electronically stored information that has been lost, damaged, altered, or overwritten as the result of the routine, good faith operation of an electronic information system" [*CCP § 2031.060(i)(1)*]. The leading federal case law on the obligation to preserve ESI also recognizes that requiring a corporation to "preserve every shred of paper, every e-mail or electronic document, and every backup tape ... would cripple large corporations ... that are almost always involved in litigation" [*Zubulake v. UBS Warburg LLC* (SDNY 2003) 220 FRD 212, 217] .

5.05[3] Parties Still Have Duty to Preserve Potentially Relevant Information Once Litigation Is Reasonably Likely. The "good faith" requirement of *CCP § 2031.060(i)(1)* means that counsel and clients cannot use the safe harbor to allow destruction of ESI that could reasonably be preserved through a targeted litigation hold. "This subdivision shall not be construed to alter any obligation to preserve discoverable information" [*CCP § 2031.060(i)(2)*]. The interplay between *CCP § 2031.060(i)(2)* and *CCP § 2031.060(i)(1)* is not yet the subject of a reported decision. However, the balance between preservation and routine destruction struck in the federal *Zubulake* case is instructive,

and may provide the basis for a reasonably defensible strategy for preserving ESI. "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*" [*Zubulake v. UBS Warburg LLC* (SDNY Oct 2003) 220 FRD 212, 217] .

5.05[4] When Duty to Preserve Arises. Federal courts have held that the obligation to preserve evidence arises when the 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* (SDNY 2003) 220 FRD 212, 216 ("*Zubulake IV*")]. A party need not specifically request that the opposing party preserve documents in order to trigger the opponent's duty to preserve. Nevertheless, counsel should consider sending a preservation demand to the opposing party, or potential parties, if there is reason to suspect that electronically stored information may be lost or destroyed. A well-crafted preservation demand can also make it easier to convince a court that any destruction of evidence occurring after the opponent has received the letter was willful [see 5.08].



Cross Reference:

Examples of when duty to preserve arises, see 13.04[3].



155 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

II. PRESERVING CLIENT'S OWN ELECTRONICALLY STORED INFORMATION

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.06

AUTHOR: Ernst Halperin, Practice Consultant

5.06 Counsel Should Develop Plan for Preservation of Client's ESI.

5.06[1] Counsel Should Consider Whether Engaging an ESI Consultant Would Be Appropriate. An ESI consultant who specializes in electronic discovery can provide assistance in designing and implementing an effective process for identifying, preserving, collecting, filtering, reviewing and producing ESI.

Consider:

An ESI consultant should have the capability to help counsel and the client develop and implement a well-targeted and defensible litigation hold that preserves data without excessively interfering with the operations of the client's organization. The consultant also should have the capability to implement a program that collects ESI without altering necessary metadata, allows review of the information and redaction of privileged matter, and maintains a chain-of-custody and audit trail of who had access to the data and when. The consultant should have experience working with the types of data systems found in the client's organization.

Hiring an ESI consultant can be especially important when the client lacks the expertise to preserve ESI, collect ESI for analysis and review without altering it, or to implement a proper chain-of-custody process. However, costs for an ESI consultant can be significant, depending upon the services they perform. Nevertheless, in the long run, hiring an ESI consultant may save money in avoided discovery disputes and the creation of a more streamlined and targeted ESI collection and analysis process.



Warning:

It is a good idea to request that the ESI consultant perform a conflict check before retention, to confirm that the consultant is not currently engaged by the opposing counsel or opposing party.

5.06[2] Data Retention Policy Is a Good Introduction to Client's Systems. If the client has a data retention policy, that policy can serve as a quick introduction for outside counsel to the client's data systems. A well written policy will have been tailored to the organization's individual needs. It will discuss types of data and their retention

schedules.



Cross Reference:

Discussion of data retention and destruction policies, see Ch. 16, Establishing Best Practices Regarding Electronically Stored Information.

5.06[3] Network Diagrams Help Counsel Understand Client's Data Environments. The client's information technology network administrator can often provide counsel with a general network diagram. The network diagram should depict the types and locations of information servers throughout the organization, and how they are interconnected. Counsel can use the network diagram as a roadmap and graphic checklist to learn from the client's IT personnel what kinds of data are stored on each server, what departments or individuals they serve, and what structure exists to tie the data on the servers to the departments or individuals.

5.06[4] Counsel Should Meet With Client's In-House Counsel, IT Personnel, and ESI Consultant to Understand Client's Data Systems, ESI Retention Practices, and Backup Technology. The first step in implementing a plan to preserve ESI is to understand the client's ESI retention policy and the actual practices within the organization. Next, using the client's retention policy and network diagram, counsel can work with the client's in-house IT personnel to identify what storage media are associated with the ESI of key players in the litigation and other witnesses likely to have ESI which should be preserved. Understanding how individuals within the client's organization perform their duties will enable counsel to determine where their ESI is stored on the network. Understanding the retention periods for ESI such as e-mails enables counsel to determine how the standard practices for e-mail retention and disposal must be modified in order to comply with the duty to preserve ESI.

After counsel has studied the client's data retention policy and reviewed the client's network diagram, counsel should hold a meeting with the client's in-house counsel, IT personnel, and any retained ESI consultant. This meeting has two purposes:

- To assist in the creation of a reasonable and defensible litigation hold.
- To identify the ESI that must be preserved for later discovery in the pending or instant litigation matter.

Having a meeting ensures that everybody involved understands the process and enables the participants to anticipate likely problem areas. The meeting should preferably occur in person, but can also be done via conference call.

Topics counsel should cover during the meeting are:

- Overview of the client's data systems.
- Identification of witnesses (custodians) who are likely to have evidence relevant to the litigation that should be preserved, and the data systems that hold their ESI.
- Identification of the types of ESI that the custodians are likely to have and where the data are located.
- Identification of databases or other structured data systems likely to hold data that should be preserved.
- Identification of any legacy data systems that are no longer in use, but which might contain evidence relevant to the subject matter of the litigation.

- Discussion of a methodology for implementing the litigation hold.
- Planning for how custodians' ESI will be collected once the opposing side issues the inevitable request for production.
- Timing and deadlines to the extent they can be anticipated.

There are additional topics that one will want to cover with in-house counsel and the ESI consultant, but do not always require in-house IT personnel's involvement.

- Planning for handling the ESI that the opponent will produce in response to any requests for production to the opponent.
- Budget for gathering and processing ESI.
- Methodology for filtering ESI once it has been gathered in order to reduce it to a manageable size for review.
- Systems for reviewing and, when necessary, redacting the filtered ESI prior to production, and for creating privilege logs.



Cross References:

Discussion of understanding the client's data systems, see *Ch. 9, Gathering and Producing Electronically Stored Information, 9.11.*

Form:

Client interview *checklist, Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferring, and Case Management Conference, 5.27.*

5.06[5] Preserving Individual Custodians' Active Data From Routine Destruction. Active data is data that employees of the company routinely access while performing their duties. Active data residing on the network that is likely to be relevant to the litigation must be preserved in order to prevent spoliation of evidence claims. In larger companies or companies in high-tech industries, some IT departments have software allowing the IT department to remotely access the contents of computers when they are connected to the client's network. This software may be used to search and/or gather data from laptops and other machines located all over the network. Without such software, data may need to be gathered from individual custodians at their computers.

Company networks often have storage capacity constraints for their active data. Companies deal with these capacity restraints by implementing data retention policies calling for the routine deletion of certain categories of active ESI on stated intervals.

The meeting with in-house counsel and the client's IT personnel will enable the project team to identify the types of data that should be preserved, which custodians have access to the data, and on which parts of the client's network the data are located. Using the client's data retention policy, the meeting participants can identify which of the data residing on the client's network are scheduled for routine deletion, and make provisions to suspend deletion of that data

Strategic Point--E-Mail Issues:



The most common area of concern is the individual users' e-mail accounts. Many systems are configured with size limits on individual accounts. The systems may be set up to routinely delete sent e-mails older than a certain number of days on a periodic basis in order to save server storage space. Individual users often also delete older e-mails in order to free up storage space.

Individual custodians should be instructed as part of the litigation hold to stop deleting e-mails. Equally important, the settings for the key individuals' e-mail accounts should be modified so that e-mails are no longer automatically deleted for the duration of the litigation hold.

Form:

See 5.26, Sample Document Preservation Memorandum.

5.06[6] Developing and Implementing Plan for Preserving Data From Structured Data Systems. At the meeting with in-house counsel and the client's IT personnel, the participants should examine to what extent information from structured data systems (such as accounting or enterprise software system databases) is likely to play a role in the case. The time periods during which relevant data was possibly created should be determined. Using the client's data retention policy, the participants can then determine whether any of the information from the relevant time periods is slated for destruction during the anticipated duration of the litigation. If so, provisions can be made to suspend the destruction of this data.

Form:

See 5.26, Sample Document Preservation Memorandum.

5.06[7] Dealing With Archived Data.

5.06[7][a] Organizations Generally Rotate Disaster Recovery Backup Media on Periodic Basis. Most organizations of any size reuse disaster recovery backup media on a rotating basis. Otherwise, the costs of storing and managing the media would be too great. Backup tape is the traditional medium used for disaster recovery. However, as the price of hard disk server space has fallen, disk-based backup systems are becoming more popular. Backup tapes get reused, while disk-based backup systems allow periodic overwriting of the disk space by new data.

Whether the client relies on traditional magnetic tape media or new disk-based systems, the organizations will typically periodically overwrite old data with new data on a schedule. In the case of backup tape data, the schedule for servers holding application programs is often different from the schedule for servers holding data created by users.



Cross Reference:

Document retention and destruction policies generally, see *Ch. 16, Establishing Best Practices Regarding Electronically Stored Information, 16.03-16.06*.

5.06[7][b] Federal Case Law Provides Guidance on Dealing With Archival Media. The leading federal case law on the issue of dealing with archival media was decided in the context of backup tapes [*Zubulake v. UBS Warburg LLC (SDNY 2003) 220 FRD 212* ("Zubulake IV")]. In the intervening six years, disk-based backup systems are becoming more popular as the price of hard-disk server space has fallen. Nevertheless, the principles enunciated in the *Zubulake IV* case are instructive, whether the client's principal archival medium is disk or magnetic tape.

The court in *Zubulake IV* recognized two categories of tapes: backup tapes that are actively used for information retrieval ("accessible backup tapes"), and backup tapes typically maintained solely for the purpose of disaster recovery ("inaccessible backup tapes") [*Zubulake v. UBS Warburg LLC (SDNY 2003) 220 FRD 212, 217*]. Accessible backup tapes likely to contain ESI relevant to the litigation should be taken out of any routine reuse cycle and preserved [*Zubulake v. UBS Warburg LLC (SDNY 2003) 220 FRD 212, 217*].

"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), and they may continue to be recycled on the schedule set forth in the company's policy. The exception to the general rule that disaster recovery tapes which are not actively used for information retrieval may continue to be recycled is if a company can identify where particular employee documents are stored on backup tapes, then the tapes storing the documents of 'key players' to the existing or threatened litigation should be preserved if the information contained on those tapes is not otherwise available. This exception applies to all backup tapes" [*Zubulake v. UBS Warburg LLC* (SDNY 2003) 220 FRD 212, 217] .

5.06[7][c] Taking a Complete Set of Backup Media Out of Reuse Cycle Is Generally Prohibitively Expensive.

The cost of taking a complete set of backup media out of the reuse cycle can be prohibitively expensive, especially in a large organization. This is likely to be true even when the backup medium is magnetic tape. Moreover, backup systems often do not allow segregation of data by certain custodians; thus, finding a particular custodian's e-mail requires restoring data for the entire company, which can be a very large expense. The client's initial reaction to a suggestion to save backup media therefore is likely to be negative. The court in *Zubulake IV* recognized this problem when it stated that backup tapes utilized solely for disaster recovery generally need not be subject to a litigation hold [*Zubulake v. UBS Warburg LLC* (SDNY 2003) 220 FRD 212, 217] .

Nevertheless, counsel should explore with the client's IT personnel whether it would be feasible to identify and remove from the rotation a subset of tapes containing backup data from the key witnesses, and whether preserving backup tapes would be merely duplicative or would preserve relevant information that is not elsewhere available on active computers. If counsel and the client decide not to set aside and preserve backup tapes due to unreasonable burden and expense, counsel should be ready to get an agreement from opposing counsel and/or a court order approving this decision.

5.06[7][d] Proper Understanding of Client's Disaster Recovery Backup Systems Allows Targeted Removal of Media From Reuse Cycle. Understanding the client's backup methodology allows counsel to determine whether the client has a responsibility to take backup media out of the reuse cycle. The client's IT personnel can help counsel to develop a proper understanding of the client's data architecture and backup regime, and whether it is feasible to remove particular backup tapes containing information of key witnesses from the reuse cycle. Equally important, if it is not possible, a thorough understanding of the client's systems will enable counsel to defend a decision not to take tapes out of the reuse cycle in the event of a spoliation claim by one's opponent.

Strategic Point:



The cost and scope of backup system discovery can be very significant, cost-shifting is a possibility, and disagreements about backup tapes are common. Accordingly, resolving what should be done with backup tapes or disks should be an early priority in the case. These topics should be addressed in ESI meet and confer sessions pursuant to Rule 3.724, and if necessary, with the court in a case management order.

5.06[8] Developing and Implementing Plan for Preservation of ESI Located off Client's Network.

5.06[8][a] Individual Custodians Often Have Important Data Stored off Network Servers. Many organizations use a server-based centralized network system for storing documents as well as a centralized e-mail server system. However, individual key witnesses often will have important data located on the personal computers they use for work. This is especially true when the primary personal computer utilized by employees is a laptop.

Strategic Points:



- **Actual Practice vs. Organization Policies.** When interviewing key custodians, counsel should determine how they actually work with their computer and the client's systems. Counsel should not merely assume that everybody's individual procedures are consistent with organizational policies.

- **E-Mail Client Systems.** E-mails systems that have an e-mail client (such as Outlook) residing on the user's computer may not be completely synchronized at any given time. The offline local copy of a remote e-mail database that has not been synchronized with the master will have information that is not on the e-mail server.

- **E-Mail Archive Files.** Another common issue is that custodians in companies with e-mail size storage limits often create individual archive files of old e-mail. The Outlook client allows users to easily create these archive files (identifiable by their extension ".PST"), and users may have multiple backup files on their hard drives or stored on other media such as a CD-ROM. These individual archive PST files likely contain data that is no longer on the central e-mail system. Counsel should determine whether the key custodians have been engaging in this practice. If so, the individual PST files should be collected and preserved.

- **Hard Drive Storage.** Custodians might also store work-related files directly on their hard drive, thereby bypassing the client's document management system. This practice is especially likely to occur in organizations in which a laptop is the custodian's primary computer and the custodian travels frequently. Again, this data should be collected and preserved.

5.06[8][b] Copying ESI Stored on Home Computers of Key Custodians May Be Warranted. Counsel's interviews with key custodians will reveal how they work, if they work at home. When custodians work at home, counsel should determine whether they use their own computers, or whether they bring home a work laptop.

When custodians work at home on their own computers, counsel should explore with them what responsive ESI might reside on their computers. This discussion must be handled carefully and with sensitivity. Home computers are likely to contain large amounts of private information (banking records, for instance), and custodians may be legitimately uncomfortable with the idea of granting access to the computer to strangers. The issue can be ameliorated somewhat if the client has a company policy in place warning employees that electronic data belongs to the company, and that a document subpoena or request for production in litigation may require collection of the information from any computer on which it is placed.

Example:

In a wrongful termination suit, the employer was allowed to inspect a former employee's company computer used at home when the employee had consented to employer policy allowing inspection of computer [*TBG Ins. Servs. Corp. v. Superior Court* (2002) 96 CA4th 443, 117 CR2d 155] .

5.06[8][c] Arranging to Copy Custodians' Off-Network Media. Counsel's interviews with document custodians will reveal sources of off-network media where ESI is stored. Flash drives, Blackberry devices, and smart phones can all have relevant data stored on them. Arrangements should be made to have the data copied from these devices.

5.06[9] Counsel and Client Should Develop and Implement Plan for Preservation of ESI Located on Legacy Software Systems. During the meeting with in-house counsel and the client's IT personnel, counsel should discuss whether any ESI may currently exist from legacy software systems that are no longer in use.

Example:

Examples might include a switch of e-mail systems from Lotus Notes to Microsoft Outlook, or a switch from a PeopleSoft enterprise software system to an Oracle system.

ESI from legacy software that may contain information relevant to the lawsuit should be preserved throughout the anticipated duration of the lawsuit.

Counsel should explore with the client's IT personnel and any retained consultant whether, and if so, how, the old data from legacy software systems can be retrieved for review and production. With this information counsel and the client together can develop a position concerning whether the source of the ESI is not reasonably accessible because of undue burden or expense.



Warning:

If counsel and the client determine that data from legacy systems will not be searched because it is not reasonably accessible, counsel will need to identify in its response to a request for production, "the types or categories of sources of electronically stored information that it asserts are not reasonably accessible" [CCP § 2023.210(d)]. The responding party preserves any objections it may have relating to that ESI by objecting and identifying information of a type or category of source that is not reasonably accessible.



Strategic Point:

Retrieving ESI from legacy data systems may require translation of the data into a usable format. It is possible that the reasonable cost of such translation may be shifted to the demanding party pursuant to *CCP § 2031.280(e)* ("[i]f necessary, the responding party at the reasonable expense of the demanding party shall, through detection devices, translate any data compilations included in the demand into reasonably usable form").

5.06[10] Counsel Should Decide Whether Imaging of Hard Drives May Be Necessary. A computer's residual-deleted electronically stored information is overwritten and lost whenever a computer is processing data. One can preserve this data by make an image copy of the hard drive, preserving all files as of a certain point in time.

A party ordinarily would not be required to take these extraordinary steps to prevent overwriting because they can involve substantial cost and burden. However, when the fact that evidence was on the hard drive itself is important (usually in trade secret cases), or when there may be questions of whether custodians have attempted to destroy evidence, preservation of the evidence may be required. In some instances, a court may issue an order requiring creation of a digital copy of the evidence [see, e.g., *Covad Communs Co. v. Revonet, Inc.* (DDC 2009) 258 FRD 5 ; *Dodge, Warren & Peters Ins. Services, Inc. v. Riley* (2003) 105 CA4th 1414, 1417-1418, 130 CR2d 385] .



Cross Reference:

Discussion of how electronic evidence is stored, and recovery of stored documents, see Ch. 1, Understanding Electronic Evidence.



Strategic Point:

Restoring deleted ESI may require translation of the data into a usable format. It is possible that the reasonable cost of such translation may be shifted to the demanding party pursuant to *CCP § 2031.280(e)* ("[i]f necessary, the responding party at the reasonable expense of the demanding party shall, through detection devices, translate any data compilations included in the demand into reasonably usable form").



156 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

II. PRESERVING CLIENT'S OWN ELECTRONICALLY STORED INFORMATION

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.07

AUTHOR: Ernst Halperin, Practice Consultant

5.07 Advising Client of Duty to Preserve.

5.07[1] Disseminating Document Preservation Memos. Counsel has a duty to effectively communicate to the client what discoverable information must be preserved. *Zubulake v. UBS Warburg (SDNY 2004) 229 FRD 422, 439* provides a roadmap of how to comply with the duty:

"[C]ounsel has a duty to effectively communicate to her client its discovery obligations so that all relevant information is discovered, retained, and produced. In particular, once the duty to preserve attaches, counsel must identify sources of discoverable information. This will usually entail speaking directly with the key players in the litigation, as well as the client's information technology personnel. In addition, when the duty to preserve attaches, counsel must put in place a litigation hold and make that known to all relevant employees by communicating with them directly. The litigation hold instructions must be reiterated regularly and compliance must be monitored. Counsel must also call for employees to produce copies of relevant electronic evidence, and must arrange for the segregation and safeguarding of any archival media (e.g., backup tapes) that the party has a duty to preserve.

"Once counsel takes these steps (or once a court order is in place), a party is fully on notice of its discovery obligations. If a party acts contrary to counsel's instructions or to a court's order, it acts at its own peril."



Warning:

Merely giving a general admonition to the client to preserve "relevant" documents is not enough, because custodians often do not understand what will be relevant. Counsel must tell the client the subject matter and the kind of documents to preserve [*Samsung Elecs. Co. v. Rambus Inc. (ED Va 2006) 439 F Supp2d 524, 565*].

After meeting with the client's IT personnel, counsel should confirm in writing what information the IT personnel will preserve on the network, and what archival media will be taken out of the reuse cycle and preserved. Counsel should

also prepare a "litigation hold" memorandum for the client to issue to all custodians whose ESI should be preserved. The litigation hold memorandum should require the custodians to acknowledge that they have received it, understand it, and will comply with the memorandum's instructions.

If the opposing party has issued a written preservation demand, the litigation hold memorandum should incorporate the specifics of the demand received from the opposing party.

Cross Reference:

Form, Sample Document Preservation Memorandum, 5.26

5.07[2] Counsel Should Disseminate Periodic Document Preservation Reminders. Counsel cannot simply rely upon the initial litigation hold memorandum. "The litigation hold instructions must be reiterated regularly and compliance must be monitored" [*Zubulake v. UBS Warburg (SDNY 2004) 229 FRD 422, 439* ("*Zubulake V*")]. Each of the document preservation reminders should repeat the instructions in the prior litigation hold. The custodians should be required to acknowledge that they have received the reminder, understand it, and will comply with its instructions. The court in *Zubulake V* admonished that counsel should take some or all of the following steps, as needed, to ensure ongoing compliance with the preservation duty [see *Zubulake v. UBS Warburg, LLC (SDNY 2004) 229 FRD 422, 433-434*] :

- Have the client re-issue litigation hold instructions periodically so that new employees are aware of it, and so it is fresh in the minds of all employees.
- Communicate directly with the key players in the litigation who are most likely to have relevant information to determine how they stored information, to verify that they understand the duty to preserve, and to instruct them not to alter or delete e-mails or other documents they created and control.
- Instruct all employees to produce electronic copies of their relevant active files.
- Make sure that all backup media the party is required to retain is identified and stored in a safe place.
- Consider taking possession of backup media so that it is not inadvertently recycled.
- Periodically monitor information technology personnel who are implementing the client's backup procedures, recycling policy, and retention and disposition policies, to determine that they are following the litigation hold.

5.07[3] Litigation Hold Software Can Be Used in Larger Organizations. Large organizations with many geographically dispersed employees present unique challenges when attempting to implement and monitor an effective litigation hold strategy. These organizations also tend to be involved in many cases at a given time. For this type of client, enterprise-wide software solutions that allow counsel to remotely implement a litigation hold on networked data have been developed.

Automated litigation hold software helps counsel identify potential custodians and automates the process of issuing legal hold messages to custodians, receiving their acknowledgments, and issuing reminders. In certain cases they can also "lock down" data on individual custodians' desktop and laptop machines, and allow individual custodians to manually select additional data files for preservation.

5.07[4] Counsel Should Confer With Document Custodians Periodically to Confirm That Documents Are Being Preserved. Counsel's obligation to ensure that relevant documents are preserved does not end once a litigation hold is in place. Rather, counsel must oversee compliance with the litigation hold, monitoring the party's effort to

identify and retain relevant information [*see Zubulake v. UBS Warburg, LLC (SDNY 2004) 229 FRD 422, 432*] .

5.07[5] Consider Whether to Inform Opposing Counsel About Preservation Efforts in Order to Head Off Later Assertion That Measures Were Inadequate. Disagreements about ESI preservation efforts are among the most contentious discovery disputes, with very high stakes. The consequences of losing a fight in which the client has been accused of spoliation can be dire if the material is deemed to be critical to the case.

Example:

A California federal district court issued an order granting an issue sanction against a party who failed to preserve ESI because it was likely that e-mails were lost when "employees were never adequately instructed as to what was relevant or how to search for such material when responding to discovery thereafter" [*Google, Inc. v. American Blind & Wallpaper Factory, Inc. (ND Ca 2007) US Dist LEXIS 48309, *16*].

 Cross Reference:

Discussion of sanctions, see Ch. 14, Seeking or Opposing Sanctions for Noncompliance.



Strategic Points:

- Making adequate efforts to identify sources of relevant information, communicating with the client's employees how and where the ESI is likely to reside, and preserving potentially responsive ESI will go a long way towards preventing a spoliation motion from succeeding.
- Counsel should also consider whether it would be advantageous to communicate with opposing counsel (beginning with initial case management meet and confer sessions under *Cal Rules Ct, Rule 3.724*) what preservation measures are being undertaken, so that opposing counsel will have trouble later complaining that they were inadequate. Doing so can potentially flush out any objections from opposing counsel before data has been destroyed. However, communicating with opposing counsel may raise awareness of an issue that counsel might not want to litigate, and that an opponent might not otherwise spot. The decision is a tactical one that counsel should consider carefully.

 Cross Reference:

Form, Sample Letter to Opposing Counsel Regarding Document Preservation Steps Taken, 5.32.



157 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

II. PRESERVING CLIENT'S OWN ELECTRONICALLY STORED INFORMATION

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.08

AUTHOR: Ernst Halperin, Practice Consultant

5.08 Consequences of Failure to Preserve.

5.08[1] Counsel Should Beware of Consequences of Failure to Preserve.

5.08[1][a] Sanctions for Spoliation of Evidence May Result. Both a party and the party's attorney may be sanctioned for spoliation of evidence. Spoliation of evidence is the destruction or significant alteration of evidence or the failure to preserve evidence for another's use in pending or future litigation [*Williams v. Russ* (2008) 167 CA4th 1215, 1223, 84 CR3d 813 (sanctions for allowing files to be destroyed during litigation); *R.S. Creative v. Creative Cotton* (1999) 75 CA4th 486, 89 CR2d 353 (terminating sanctions appropriate for forging contract and deleting computer files)].

Although there is no tort cause of action for the intentional destruction of evidence after litigation has commenced [see *Cedars-Sinai Medical Center v. Superior Court* (1998) 18 C4th 1, 12, 74 CR2d 248, 954 P2d 511], destruction of evidence is considered a misuse of the discovery process that is subject to a broad range of sanctions [*Williams v. Russ* (2008) 167 CA4th 1215, 1223, 84 CR3d 813; see CCP §§ 2023.010(d), 2023.030(a)-(d)]. Sanctions imposed for spoliation of evidence include [see *Cedars-Sinai Medical Center v. Superior Court* (1998) 18 C4th 1, 11-13, 74 CR2d 248, 954 P2d 511; see also CCP § 2023]:

- An evidentiary inference that the destroyed evidence was unfavorable to the party that caused its destruction [see *Evid Code* § 413].
- Monetary sanctions.
- Contempt.
- Issue sanctions ordering that designated facts be taken as established or precluding the offending party from supporting or opposing designated claims or defenses.

- Evidence sanctions prohibiting the offending party from introducing designated matters into evidence.
- Terminating sanctions including striking part or all of the pleadings, dismissing part or all of the action, or granting a default judgment against the offending party.
- Misdemeanor criminal penalties [*see Pen Code § 135*].

In addition, State Bar disciplinary sanctions can be imposed on attorneys who participate in the spoliation of evidence [*see Cedars-Sinai Medical Center v. Superior Court (1998) 18 C4th 1, 12, 74 CR2d 248, 954 P2d 511*] .

Cross Reference:

Discussion of sanctions for spoliation, see *Ch. 13, Seeking or Opposing Sanctions for Noncompliance, 13.03-13.10*.

5.08[1][b] Severity of Sanction Is Determined by Culpability and Degree of Prejudice. Sanctions must be proportionate to the offending party's misconduct [*see McGinty v. Superior Court (1994) 26 CA4th 204, 210-212, 31 CR2d 292*] . Accordingly the more egregious the spoliation, the more severe the sanction imposed, with a terminating sanction usually being reserved for intentional destruction of material evidence that the innocent party needs to prove its case [*see Williams v. Russ (2008) 167 CA4th 1215, 1223, 84 CR3d 813*] .

Cross Reference:

Discussion of types of sanctions available, see *Ch. 13, Seeking or Opposing Sanctions for Noncompliance, 13.08*.

5.08[2] Opposing Party May Seek Injunction to Protect Against Destruction of Electronic Evidence. As an alternative, or in addition to, sanctions, it may be possible for the opposing party to obtain an injunction requiring preservation of electronic evidence if the requesting party can show likelihood of irreparable harm.

Example:

In a trade secret case involving employees of an insurance brokerage firm who took electronic data with them when they left to set up a competing brokerage, a California appellate court affirmed a superior court injunction prohibiting the departing employees from destroying, deleting, or hiding any of their electronic storage media, and requiring them to allow court-appointed experts to copy all of it, recover lost or deleted files, and perform automated searches [*see Dodge, Warren & Peters Ins. Services, Inc. v. Riley (2003) 105 CA4th 1414, 130 CR2d 385*] .

Cross References:

Discussion of obtaining protective order against spoliation of electronic evidence, see *Ch. 11, Seeking or Opposing Protective Order, 11.03-11.07*.

If there is risk of purposeful destruction, court may order collection and preservation of ESI by neutral expert, see *Ch. 9, Gathering and Producing Electronically Stored Information, 9.27*.

5.08[3] Counsel Should Review Possible Consequences With Client. Informing the client of the possibility of sanctions may deter willful destruction of electronically stored information. In particular, the client should be warned against destroying documents that support the opposing party's claims or defenses. Counsel must impress upon the client that sanctions for intentional destruction of evidence can be costly both monetarily and in regard to presentation of the merits of the case.



158 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

III. NOTIFYING OPPOSING PARTY THAT E-DISCOVERY WILL BE SOUGHT

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.09

AUTHOR: Ernst Halperin, Practice Consultant

5.09 CHECKLIST: Notifying Opposing Party That E-Discovery Will Be Sought.

☐ Send preservation demand as soon as possible:

☐ As soon as possible after complaint is filed, if it is apparent from the inception that e-discovery will be involved.

☐ Even before complaint is filed, if concern exists that relevant ESI may be destroyed in interim period.

☐ At any subsequent time when it becomes apparent that e-discovery will play role in litigation.

Discussion:

See 5.11.

☐ Prepare notice stating:

Discussion:

See 5.12.

Form:

See 5.28

☐ Fact that litigation has been commenced or is imminent.

- ☐ General statement of type of evidence claimed to be relevant to claims and defenses.
 - ☐ A demand that all ESI relevant to that stored information be preserved.
 - ☐ A demand that any routine destruction policies that might be applicable to that evidence be immediately suspended.
- ☐ Send preservation demand to opposing party.

Discussion:

See 5.13



159 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

III. NOTIFYING OPPOSING PARTY THAT E-DISCOVERY WILL BE SOUGHT

*1-5 MB Practice Guide: CA E-Discovery and Evidence 5.10***AUTHOR:** Ernst Halperin, Practice Consultant**5.10 Options and Strategy for Notifying Opposing Party.**

Counsel should formally initiate the e-discovery process by giving the opposing party a "preservation demand" informing the opposing party that all evidence relevant to the subject matter of the litigation should be retained, and any routine document destruction policies should be suspended. Although this notice is not *required* by law, there are sound reasons why the process should be initiated in this manner. The preservation demand is intended to assure that any ESI needed to prove the demanding party's case will be available at trial by putting the opposing party on notice that the evidence may be needed in the litigation and that any further destruction of potential evidence may result in sanctions for spoliation of evidence. Such a notice establishes a "paper trail" for preservation if a motion for sanctions becomes necessary later in the litigation.

Example:

A preservation demand is a factor the court may consider in sanctioning a party that ignores the demand and destroys documents [see, e.g., *Lombardo v. Broadway Stores (Cal App 4th Dist 2002) 2002 Cal App Unpub LEXIS 4700, 1-2* (defendant sanctioned for destroying computer form of payroll evidence sought by plaintiff after plaintiff had sent letters demanding preservation of evidence)].

**Strategic Point--Plan for Reciprocal Demands:**

ESI negotiations often involve an aspect of "What is good for the goose is good for the gander" in that preservation demands or demands for production of ESI will often provoke a reciprocal demand from the other party. Thus, before sending a preservation demand that specifies certain types of ESI that should be preserved, counsel should confirm that his or her own client is preserving the same type of ESI and is willing to produce it. For example, although there may be factors that justify different approaches for differently situated parties, a court may well expect that a party demanding search and production from backup tapes should be willing to do the same.

**Strategic Point--Injunction May Be Sought If Destruction of ESI Is a Concern.**

If counsel believes that a preservation demand may be insufficient to ward off destruction of ESI in an opponent's possession, or, worse yet, that it may actually trigger the illegal destruction of such evidence, an injunction against destruction of relevant ESI also may be sought [see *Dodge, Warren & Peters Ins. Services, Inc. v. Riley* (2003) 105 CA4th 1414, 130 CR2d 385] .

 Cross References:

Discussion of meet and confer obligations, see 5.14-5.25.

Sanctions for spoliation of evidence, see Ch. 13, Seeking or Opposing Sanctions for Noncompliance.

Injunctions to preserve ESI, see Ch. 7, Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery.



160 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

III. NOTIFYING OPPOSING PARTY THAT E-DISCOVERY WILL BE SOUGHT

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.11

AUTHOR: Ernst Halperin, Practice Consultant

5.11 Preservation Demand Initiates E-Discovery.

The party seeking e-discovery should begin by sending a preservation demand to the other party. Preservation demands can be sent before a complaint has been filed, and are often a component of a plaintiff's demand letter to a defendant. They can also be sent after commencement of litigation, once it becomes evident that e-discovery will be conducted in the case.

Strategic Point:



If the preservation demand is given before the complaint is filed, as discussed above, it may be combined with a traditional pre-lawsuit "demand letter."



Cross Reference:

Form, preservation demand combined with traditional demand letter, see 5.28.



161 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

III. NOTIFYING OPPOSING PARTY THAT E-DISCOVERY WILL BE SOUGHT

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.12

AUTHOR: Ernst Halperin, Practice Consultant

5.12 Counsel Must Prepare Preservation Demand.

Counsel must prepare the preservation demand notice to be sent to the opposing party. The preservation demand notice should include the following:

- The fact that litigation has been commenced or is imminent.
- A general statement of the type of evidence claimed to be relevant to the claims and defenses.
- A demand that all ESI relevant to that stored information be preserved.
- A demand that any routine destruction policies that might be applicable to that evidence be immediately suspended.

Cross Reference:

Form, preservation demand combined with traditional demand letter, see 5.28.



162 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

III. NOTIFYING OPPOSING PARTY THAT E-DISCOVERY WILL BE SOUGHT

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.13

AUTHOR: Ernst Halperin, Practice Consultant

5.13 Counsel Must Send Preservation Demand to Opposing Party.

Counsel must send the preservation demand to the opposing party to the action. There is no required method for sending notice but a written confirmation of receipt is recommended. Formal service is not required.



163 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

IV. MEETING AND CONFERRING REGARDING E-DISCOVERY

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.14

AUTHOR: Ernst Halperin, Practice Consultant

5.14 CHECKLIST: Meeting and Conferencing Regarding E-Discovery

- ☐ Negotiate with other parties to set time, date, manner and location for all parties to meet and confer regarding e-discovery

Authority:

Cal Rules Ct, Rule 3.724(8)

Discussion:

See 5.16, 5.16A

- ☐ Must occur no later than 30 calendar days before date set for initial case management conference.
- ☐ May be in person or by telephone.
- ☐ May be separate or combined with meet and confer to discuss non-ESI issues.

- ☐ Prepare to meet and confer regarding ESI.

Discussion:

See 5.18

- ☐ Prepare carefully and thoroughly.

Discussion:

See 5.18[1]

- ☐ Consult technical personnel on technical issues.

Discussion:

See 5.18[2]

- ☐ Analyze document request if one has been served.

Discussion:

See 5.18[3]

- ☐ Consult with team and determine what specific issues relating to discovery of ESI are likely to need resolution.

Discussion:

See 5.18[4]

- ☐ Discuss following issues at conference:

Authority:

Cal Rules Ct, Rule 3.724(8)

Discussion:

See 5.19[1]]

Form:

See 5.30 (meet and confer checklist)

- ☐ Preservation of information.

Discussion:

See 5.19[2].

- ☐ Form or forms in which information will be produced.

Discussion:

See 5.19[3]

- ☐ Time within which information will be produced.

Discussion:

See 5.19[4]

- ☐ Scope of discovery of electronically stored information.

Discussion:

See 5.19[5]

- ☐ Method for asserting or preserving claims of privilege or attorney work product.

Discussion:

See 5.19[6]

- ☐ Method for asserting or preserving the confidentiality, privacy, trade secrets, or proprietary status of information.

Discussion:

See 5.19[7]

- ☐ How the cost of production of electronically stored information is to be allocated among parties.

Discussion:

See 5.19[8]

- ☐ Any other issues, including development of a proposed plan for discovery of electronically stored information.

Discussion:

See 5.19[9]

- ☐ Adopt and document proposed discovery plan.

Authority:

Cal Rules Ct, Rule 3.724(8)

Discussion:

See 5.19[9]

- ☐ If opposing counsel is not forthcoming, consider propounding interrogatories or noticing a deposition.

Discussion:

See 5.19[10]

Form:

See 5.29

- ☐ Identify areas of agreement and disagreement.

- ☐ Identify areas parties can agree on.

Discussion:

See 5.20[1]

- ☐ Determine if court intervention will be necessary for unresolved issues.

Discussion:

See 5.20[2]

- ☐ Prepare and execute any formal agreements negotiated at conference.

Discussion:

See 5.21



164 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

IV. MEETING AND CONFERRING REGARDING E-DISCOVERY

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.15

AUTHOR: Ernst Halperin, Practice Consultant

5.15 Options and Strategy for Complying With Meet and Confer Requirement.

To make the most effective use of the e-discovery conference, counsel should be familiar with each of the issues that will be considered at the conference. This means that counsel needs to determine the needs of the client in relation to the discovery of electronically stored information, and formalize plans on how to achieve an agreement with the opposing party to meet these needs.

Counsel should attend the conference with a willingness to negotiate, and be persistent in working through each issue to avoid confusion and to make sure all issues are covered. After the conference, counsel should memorialize any consensus or agreements by written agreement, or better still, incorporation into a stipulated case management order.



165 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

IV. MEETING AND CONFERRING REGARDING E-DISCOVERY

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.16

AUTHOR: Ernst Halperin, Practice Consultant

5.16 All Parties Must Meet and Confer to Discuss Specified Issues.

The parties must meet and confer, in person or by telephone, to discuss the following issues at least 30 calendar days before the date set for the initial case management conference [*Cal Rules Ct, Rule 3.724(8)*]:

- Any issues relating to the preservation of discoverable electronically stored information.
- The form or forms in which information will be produced.
- The time within which the information will be produced.
- The scope of discovery of the information.
- The method for asserting or preserving claims of privilege or attorney work product, including whether such claims may be asserted after production.
- The method for asserting or preserving the confidentiality, privacy, trade secrets, or proprietary status of information relating to a party or person not a party to the civil proceedings.
- How the cost of production of electronically stored information is to be allocated among the parties.
- Any other issues related to the discovery of electronically stored information, including developing a proposed plan relating to the discovery of the information.



Strategic Point--Attendance by Counsel and IT Personnel.

Cal Rules Ct, Rule 3.724 states that "all parties must meet and confer, in person or by telephone," to consider issues related to the discovery of electronically stored information. Presumably, the actual intention is that parties' counsel meet and confer. Nevertheless, it may be useful to have a member of the client's IT personnel also attend the conference in case questions arise that are beyond the technical

competence of the lawyers.

Consider:

In addition to the e-discovery meet and confer requirement [*see* 5.18], parties are required to meet and confer to consider other issues commonly included in a case management order [*see Cal Rules Ct, Rule* 3.724].



Cross Reference:

Meet and confer requirements in non-ESI context, see Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure, Ch. 23, Case Management.



166 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

IV. MEETING AND CONFERRING REGARDING E-DISCOVERY

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.17

AUTHOR: Ernst Halperin, Practice Consultant

5.17 Counsel Must Decide Time, Manner, and Location for Meet and Confer.

5.17[1] Meet and Confer Must Occur No Later Than 30 Days Before Date Set for Initial Case Management Conference. The meet and confer must occur no later than 30 calendar days before the date set for the initial case management conference, unless the court orders another time period [*Cal Rules Ct, Rule 3.724(8)*].



Timing--Details Must Be Negotiated by Parties:

The rule of court does not state how the date, time, manner, and location for the meet and confer are to be determined. It merely says that all parties must meet within the specified time frame. Presumably the parties must decide in advance how and when the meet and confer will occur.



Timing--Meet and Confer Ideally Should Occur Prior to Discovery Demand:

Although the rules do not specify a precise order for these steps, the meet and confer normally will be conducted before a formal discovery demand is filed.



Cross References:

Filing formal demand for production of ESI, see *Ch. 6, Demanding Production of Electronically Stored Information in California Court*, 6.09-6.13.

5.17[2] Meet and Confer May Be in Person or by Telephone. The meet and confer may be held in person or by telephone [*Cal Rules of Ct, Rule 3.724*]. Presumably this means that some parties may attend in person and others by telephone, as long as all parties are present.

5.17[3] ESI Meet and Confer May Be Separate or Combined With Meet and Confer to Discuss Non-ESI Issues. In addition to the e-discovery meet and confer requirement, the parties are required to meet and confer to consider other issues commonly included in a case management order [*see Cal Rules Ct, Rule 3.724*]. The rule does not mandate that the conferences be held separately or together [*see Cal Rules Ct, Rule 3.724*]. Thus, if the parties want to

hold a single conference to discuss both sets of issues, they are free to do so. However, unless e-discovery issues in the case are minimal, it may be best to hold separate conferences, since e-discovery typically involves technical questions that are distinct from other discovery issues.



167 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

IV. MEETING AND CONFERRING REGARDING E-DISCOVERY

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.18

AUTHOR: Ernst Halperin, Practice Consultant

5.18 Counsel Must Prepare for Meet and Confer Regarding ESI.

5.18[1] Careful Preparation Is Essential. In order to effectively meet and confer about the issues that are required to be discussed, counsel will need to:

- Understand the types of ESI that will be relevant to the litigation.
- Have prepared a data preservation plan prior to the meet and confer.
- Know whether the ESI relevant to the litigation implicates privacy, confidentiality, or trade-secret concerns that would necessitate protective orders.

5.18[2] Technical Personnel Should Educate Counsel of Technical Issues. The client's IT personnel and/or an ESI consultant should be able to educate counsel about the technical aspects of these issues. Counsel should discuss each of the meet and confer topics with the client's IT personnel and any retained ESI discovery consultant in order to adequately prepare for the meet and confer.

5.18[3] Responding Parties Should Analyze Document Request If One Has Been Served. If a document request has already been served on the client, counsel should include the request in the topic of the discussion with the client's IT personnel and any retained ESI consultant, in order to develop a plan for gathering, reviewing, and producing the ESI. The discussion should include the format for the produced information, and what metadata would be included in any load files of data produced in TIFF or PDF format.

5.18[4] Counsel's Team Should Identify Issues That Are Likely to Need Resolution. While meeting with counsel's team, determine which issues relating to the discovery of electronically stored information are likely to need resolution. The following specific issues should be considered:

- If a production demand has already been issued, consider whether keyword searches could be used to identify and narrow the scope of ESI that must be reviewed [Covad Communications Co. v. Revonet,

Inc. (DDC 2009) 259 FRD 5 (parties should have cooperated to formulate key word searches)).

- Determine the form in which counsel wants electronically stored information to be produced [see 5.19[3]].
- Formulate any objections the counsel and the client have to specific forms of production [see 5.19[3]].
- If a request for production has been issued by counsel for the opposing party, define the time within which the client can realistically respond to it [see 5.19[4]].
- Inquire whether there are sources of ESI likely to contain information responsive to the issues in the litigation, but which are not reasonably accessible. This discussion should give counsel the factual basis with which to support an objection to discovery from these data sources [see 5.19[8]].
- Determine whether the respondent is likely to have any difficulty retrieving potentially relevant information [see 5.19[4]].
- Will the respondent seek cost-shifting or other allocation of the costs of production [see 5.19[8]]?
- Does the respondent need a confidentiality agreement to protect trade secrets, privacy interests, or other proprietary rights belonging to the respondent or to a nonparty to the action [see 5.19[7]]?
- Will the demanding party seek direct access to the opposing party's computers for testing or sampling, or physical production or imaging of computer hard drives [see 5.19[5]]?
- Should counsel seek an agreement that attorney-client privilege or work product protection is not waived by the inadvertent production of privileged or protected documents [see 5.19[6]].



Cross Reference:

Checklist for "meet and confer" requirement, see 5.30.



168 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

IV. MEETING AND CONFERRING REGARDING E-DISCOVERY

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.19

AUTHOR: Ernst Halperin, Practice Consultant

5.19 Parties Should Discuss Particular Issues at Conference.

5.19[1] Issues Specified in Rule of Court Must Be Considered. The participants should use the list of topics in the governing rule of court as a guide to the issues to be discussed at the meet and confer. The basic topics are set out once again below [*see also* 5.16], and discussed individually in greater detail in the subsections that follow [*Cal Rules Ct, Rule 3.724(8)*]:

- Preservation of information [*see* 5.19[2]].
- Form or forms in which information will be produced [*see* 5.19[3]].
- Time within which information will be produced [*see* 5.19[4]].
- Scope of discovery of electronically stored information [*see* 5.19[5]].
- Method for asserting or preserving claims of privilege or attorney work product [*see* 5.19[6]].
- Method for asserting or preserving the confidentiality, privacy, trade secrets, or proprietary status of information [*see* 5.19[7]].
- How the cost of production of electronically stored information is to be allocated among the parties [*see* 5.19[8]].
- Any other issues, including development of a proposed plan for discovery of electronically stored information [*see* 5.19[9]].



Cross Reference:

Checklist for "meet and confer" requirement, *see* 5.30.

5.19[2] Preservation of Discoverable Electronically Stored Information.

5.19[2][a] Counsel Should Inquire About Opposing Party's ESI Creation, Storage, Collection and Document Retention Program. At the e-discovery conference, parties should consider any issues relating to the preservation of discoverable electronically stored information [see *Cal Rules Ct, Rule 3.724(8)*]. The following questions should help elicit the types of information needed to determine if electronically stored information related to the action may be available from the opposing party:

- Who are the key document custodians?
- Where and how do the key custodians create ESI?
- What types of ESI do they create?
- What ESI has been preserved and subject to the litigation hold already?
- What kind of document management system does the opposing party maintain?
- What structured data systems such as accounting and process databases does the opposing party maintain? How are data from that system archived? How far back?
- What ESI will the opposing party claim is not reasonably accessible, and on what basis?
- What kind of e-mail system does the party have, and is that system programmed to delete e-mails automatically after a certain period of time? What is that period of time?
- What other sources of ESI does the opposing party have? Do key custodians utilize smart phones or personal digital assistants? If so, what type?
- Do the opposing party's key custodians work from home? If so, do they utilize their home computers?
- Do the opposing party's key custodians utilize portable storage media such as thumb drives, CD-ROM, or portable backup drives in their work?
- What, if any, is the party's policy for retention and disposition of electronically stored information?
- For what length of time are documents retained?
- Are documents retained other than in their native format?
- Are certain documents retained for longer periods of time, and if so, based on what criteria?
- Does the party have a backup system? If so, describe the system and how long the backup tapes or other media are maintained.
- Is the data on the backup searchable?
- Is there data on the backup system that is not available on active systems?

5.19[2][b] Counsel Should Find Out Whether Opposing Party Has Suspended Records Destruction Routine or Imposed Selective Litigation Hold. When litigation has commenced or is imminent, a party should either suspend its records destruction routine altogether or impose a selective litigation hold [see 5.06[3]]. A selective litigation hold may involve preserving the records of all key players who may have relevant information, as well as all documents related to certain topics that are the subject of the litigation:



Strategic Point:

A party to litigation need not rely on the other party's "good faith" in fulfilling its duty to preserve electronic information. Instead, the e-discovery conference should be used to learn about the other party's record retention and disposition policy, and to clarify what steps each party believes the other party should take to preserve relevant information. The following questions may be useful in gathering information relevant to document preservation:

- Were routine deletion programs suspended or kept on after suit was filed?
- If they were shut off, on what date was the program suspended?
- What efforts have been made to identify and save electronically stored information that may be relevant to this action?
- Is the party aware of the routine deletion or other destruction of any e-mails or other documents pertinent to this action?
- Who is responsible for searching for electronically stored information pertaining to this action?
- How did this person conduct the search?
- What sources of electronically stored information were searched?
- Did search include network servers, e-mails, individual hard drives?
- If individual hard drives were searched, whose were they?
- Did the search involve the use of keywords and, if so, what were they?

Consider:

Some ESI is modified and/or deleted simply by operation of a computer system. For example, in deleting a file, the Windows operating system leaves the file on the hard drive of a computer, but in time writes over this information during continued operation. Similarly, file access times maybe updated each time a file is opened. A party ordinarily would not be required to take measures to prevent overwriting of a computer's residual-deleted electronically stored information, which may occur whenever a computer is processing data [see 5.05[3][b]]. For discussion of these types of issues, see Ch. 1, Understanding Electronic Evidence.

The parties should discuss whether the issues in the case warrant the expense of preserving this information by imaging key custodians' computer hard drives.

In urgent and time-sensitive situations in which ESI is likely being destroyed, counsel will need to take steps at the very earliest stages of the litigation to preserve evidence, perhaps by seeking a preservation and ESI imaging order, rather than waiting until the meet and confer.

Cross Reference:

Court ordered collection of ESI by neutral expert, see 9.38.

Injunction to protect against destruction of ESI, see *Ch. 7, Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery*, 7.03-7.12.

5.19[3] Form in Which Information Will Be Produced.

5.19[3][a] Parties Should Address Their Rights and Duties Concerning Form of Production. Another issue for discussion at the e-discovery conference is the form or forms in which information will be produced [see *Cal Rules Ct, Rule 3.724(8)(B)*]. A party seeking discovery of electronically stored information may specify the form or forms in which the information is to be produced [CCP § 2031.030(a)(2)]. If the demand for production does not specify a form, the producing party must produce the information in the form or forms in which it is ordinarily maintained or in a form that is reasonably usable [CCP § 2031.280(d)(1)]. Unless the parties otherwise agree or the court otherwise orders, a party need not produce the same electronically stored information in more than one form [CCP § 2031.280(d)(2)].

Cross References:

Discussion of requesting form of production, see *Ch. 6, Requesting Production of Electronically Stored Information in California Court*, 6.03-6.08.

Discussion of responding or objecting to form of production, see *Ch. 8, Responding to Electronic Discovery Demands in California Court*.

Understanding the nature and characteristics of electronically stored information, see *Ch. 1, Understanding Electronic Evidence*, 1.15-1.35.

5.19[3][b] Hard Copy Production of Electronically Stored Information Is Disfavored. Electronically stored information may be produced electronically or through a printout, sometimes referred to as a "hard copy." Documents produced electronically are usually more useful than hard copy because they are often searchable by key words, sortable and filterable. For example, when the requesting party is looking through a group of documents for information about a particular topic, for example, a review of e-mails filtered to show those sent by a particular witness, sorted by date, and containing certain search words will be much quicker than a page-by-page review of hard copy.



Warning:

The "default procedures" for production of electronically stored information, which provide that if the request does not specify, the information should be produced in a form in which it is ordinarily maintained or in a reasonably usable form [see CCP 2031.280(d)(1)], have been the source of a significant number of disputes. Courts continue to wrestle with how electronically stored information is "ordinarily maintained," or what is a "reasonably usable form," but searchability and sortability are key features. The consensus seems to be that hard copies of electronically stored information ordinarily are not an acceptable form [see *L.H. v. Schwarzenegger (ED Cal 2008) 2008 US Dist LEXIS 86829* (sanctions for producing non-sortable PDF copies); *Lombardo v. Broadway Stores (2002) 2002 Cal App Unpub LEXIS 4700, 1-2* (sanctions for loss of the electronic form of payroll evidence); *Bray & Gillespie Mgmt. LLC v. Lexington Ins. Co. (MD Fla 2009) 2009 US Dist LEXIS 21250* (attorneys sanctioned for removing metadata from electronic records and producing in TIFF format when native format had been

requested)].

Examples:

- Courts have reasoned that for hard copy to be an acceptable format under the "ordinarily maintained" alternative, one would have to believe that a company, in its day-to-day operations, keeps all its electronic communications on paper [see, e.g., *Covad Communs Co. v. Revonet, Inc.* (DDC 2008) 254 FRD 147, 150].

- A party does not fulfill its duty to produce documents in a "reasonably usable form" when it produces those documents in paper format. A party's option to produce in a reasonably usable form does not mean it is free to convert electronically stored information from the form in which it is ordinarily maintained to a different form that makes it more difficult to use the information efficiently in the litigation [see, e.g., *White v. Graceland College Ctr. for Professional Dev. & Lifelong Learning, Inc.* (D Kan 2008) 586 F Supp2d 1250, 1264].



Strategic Point--All Parties:

As one court pointed out, these disputes are likely to be avoided if the parties "start abiding by their obligations" to "talk to each other about the form of production" [see *Covad Communs Co. v. Revonet, Inc.* (DDC 2008) 254 FRD 147, 149].



Cross Reference:

Discussion of form in which electronically stored information will be produced, see *Ch. 9, Gathering and Producing Electronically Stored Information*, 9.47-9.56.

5.19[3][c] Production in TIFF or PDF With Load Files Is Common. Different electronic forms for the production of electronically stored information are also available. The most common are to convert documents from their native format into PDF or TIFF format (sometimes referred to as "near paper" format), and accompany the document production with a load file of relevant data about the documents such as date/sender/recipient/file location, etc. This mode of production works well with common document review software (e.g., Concordance or Summation), and maintains the sortability and searchability of the native ESI. This method also provides images of the produced ESI that can be Bates numbered for easy reference and tracking in discovery and at trial.

However, this mode of production may make certain documents such as spreadsheets difficult to read and review, because the process of converting the spreadsheets to TIFF or PDF often changes the layout and readability of the sheet. Moreover, limiting production to TIFF or PDF with a load file will not recover metadata that would have been in a native file and that may be relevant (e.g., file access times and formulas in spreadsheets).



Strategic Point:

Federal courts sometimes refuse requests for production of ESI in native format, concluding that metadata is of limited evidentiary value, and dealing with the extra difficulties of handling native format files can waste litigation resources. However, if a party can show a particularized need for the native format, a court is likely to order production of metadata, especially if that party specifically requested that electronically stored information be produced in native format [see *Wyeth v. Impax Labs., Inc.* (D Del 2006) 248 FRD 169, 171; *Covad Communs Co. v. Revonet, Inc.* (DDC 2009) 258 FRD 5 (in suit alleging unauthorized use of a database, court allowed discovery of metadata regarding database access,

observing it was "at the heart of the case")].

 Cross Reference:

Discussion of metadata, see *Ch. 1, Understanding Electronic Evidence, 1.22[3]*.

5.19[3][d] Parties Should Establish Guidelines for Form of Production. The following questions may be useful in establishing the parties' intentions as to the form or forms for production of electronically stored information:

- Will hard copy be an acceptable form of production for any electronically stored information?
- How does each party ordinarily maintain their electronically stored information, including software and e-mail programs?
- Do parties have objections to producing documents in native format?
- Does any party know of issues in the case for which metadata may be crucial or useful to an understanding of particular documents?
- What form of production is most cost efficient for the parties?
- Do parties have software that will permit them to access information from the form in which the opposing party intends to produce electronically stored information?

5.19[4] Parties Should Establish Time Within Which Information Will Be Produced. At the e-discovery conference, parties are advised to discuss the time within which information will be produced [*Cal Rules Ct, Rule 3.724(8)(C)*].

While many productions of electronically stored information can be completed within the usual time period for responding to a discovery request, large productions or those involving technical issues will likely require extended or rolling production deadlines. For example, archived files, information on backup media, or information from a retired computer system may require additional time to collect and analyze documents relevant to discovery requests. Any such issues should be identified at the e-discovery conference, and the parties should attempt to agree on a schedule for production of such items to avoid later disputes.

In addition, the parties may need to create special discovery deadlines in large cases. Particularly in complex litigation, it may take months to process and review thousands or even millions of potentially relevant documents. The parties also may want to schedule the production of certain documents for delivery before the depositions of key players.

 Cross Reference:

Discussion of budgeting time for e-discovery processing and review in complex cases, see *Ch. 4, Planning E-Discovery, 4.15-4.18*.

5.19[5] Parties Should Attempt to Limit Scope of Discovery of ESI. Parties should discuss the scope of e-discovery at the conference [*Cal Rules Ct, Rule 3.724(8)(D)*].

A party may obtain discovery of electronically stored information in accordance with the general scope of discovery [*CCP § 2031.010(a)*]. That is, a party generally may discover any matter, not privileged, that is relevant to the subject matter of the action [*see CCP § 2017.010*]. Nevertheless, because of the vast amounts of information that can be created and stored on a computer, courts generally recognize the need for practical and reasonable limits on e-discovery. In contrast to the discovery of other types of information, courts recognize that retrieving all potentially relevant

electronically stored information may not be worth the attendant costs and burdens [see *CCP* § 2017.020 (court must limit scope of discovery if burden, expense, or intrusiveness outweighs likely benefit)].

Parties should consider the following issues in connection with the scope of discovery:

- Can discovery be limited to a particular set of key custodians who are expected to have the most relevant ESI?
- Can the scope of discovery be limited by reviewing and producing only documents that are found with an agreed set of search terms?
- Requested information must be relevant, but the burden to show lack of relevancy generally is on the party resisting discovery.
- Requested information must be non-privileged and non-protected.
- It is uncommon to allow a party direct access to the opposing party's computers.
- Direct testing or sampling of an opposing party's electronically stored information generally is not permitted.
- Physical production or imaging of computer hard drives generally is limited to situations in which the party being required to so produce has engaged in prior discovery misconduct, willful destruction of evidence, or evidence that files were on the computer or were deleted from the computer is relevant to the issues in the case (which happens most frequently in trade secret litigation).



Cross References:

Discussion of scope of production, see *Ch. 6, Requesting Production of Electronically Stored Information in California Court*, 6.05.

Discussion of limiting the scope of collection, see *Ch. 9, Gathering and Producing Electronically Stored Information*, 9.28-9.35.

5.19[6] Counsel Should Discuss Method for Asserting or Preserving Claims of Privilege or Attorney Work Product. At the e-discovery conference, parties should discuss the method for asserting claims of privilege or attorney work product, including whether such claims may be asserted after production [*Cal Rules Ct, Rule 3.724(8)(E)*].

In the absence of such an agreement, the Electronic Discovery Act provides that if ESI produced in discovery is subject to a claim of privilege or of protection as attorney work product, the party making the claim may notify any party that received the information of the claim and the basis for the claim [*CCP* § 2031.285(a)]. The Act imposes a duty on the receiving party to immediately sequester the information and either return it, or present the information to the court conditionally under seal for a determination of the privilege claim [*CCP* § 2031.285(b)]. The party challenging the claim must make a motion within 30 days of receiving the claim and presenting the information to the court conditionally under seal, and cannot use the information in any manner until the court decides the issue [*CCP* § 2031.285(d)(1), (2)].

Parties may agree that an inadvertent disclosure of a privileged or protected document produced in discovery will not waive the privilege or protection, and provide for a method to "claw back" inadvertently produced privileged information. Any such agreement should preferably be incorporated into a case-management order. It is safest to agree to use the procedure set forth in *CCP* 2031.285, because then there is statutory authority supporting the assertion that

the procedures invoked by the "clawback" agreement do not constitute a voluntary waiver of privilege.



Strategic Points--Drafting and Negotiating Stipulated Privilege Review Agreements:

- **Bring Draft Stipulation to Meet and Confer Conference.** If counsel does not like the procedure set out in *CCP § 2031.285*, he or she should draft a proposed stipulation and bring it to the meet and confer conference. If the conference is telephonic, counsel should fax it or e-mail a PDF to opposing counsel.

- **Take Charge of Drafting Stipulated Agreement:** Counsel should not send opposing counsel the word processing version of the proposed stipulation. It is better to send a PDF, and offer to amend it if it is not acceptable as proposed. That way, opposing counsel needs to ask to include changes, rather than counsel having to chase opposing counsel to put in counsel's preferred language.



Strategic Point--Stipulated Agreement Does Not Lessen Necessity for Through Privilege Review:

The fact that a party has entered into a stipulated "clawback" order does not lessen the necessity of conducting a well-designed, thorough, and implemented privilege review. Voluntary disclosure of privileged information constitutes a waiver of the communication [*Evid Code § 912(a)*]. Counsel does not want to end up in the middle of a fight about whether the privilege review conducted was so lax that any production of privileged materials was not inadvertent.

Another possible type of agreement is a "quick peek" agreement allowing the requesting party to examine all information on the condition that the producing party is not precluded from later asserting privilege or work product protection as to the information examined. Quick peek agreements entail a much higher risk that a third-party in subsequent litigation could successfully assert that the producing party waived privilege by entering into a voluntary agreement allowing a significant portion of a privileged document to be disclosed.



Cross References:

Discussion of privilege, see *Ch. 10, Opposing Request for Production of Electronic Evidence in California Court*, 10.08.

Discussion of "clawback" rule, see *Ch. 3, Ethical Issues for Attorneys in E-Discovery*, 3.14.

Additional discussion of "quick peek" agreements, see *Ch. 3, Ethical Issues for Attorneys in E-Discovery*, 3.14[1].

5.19[7] Counsel Should Discuss Stipulated Protective Order for Asserting or Preserving Confidentiality, Privacy, Trade Secrets, or Proprietary Status of Information Relating to Non-Parties. Commercial enterprises often have a host of data that is commercially sensitive, involves confidential or proprietary information, or implicates privacy concerns of one of the litigants or third parties. The parties can protect this information with a stipulated protective order regarding confidential information. Stipulated protective orders commonly do the following:

- Allow the parties to designate documents as confidential.
- Designate who is allowed to see the information.

- Limit the uses to which the recipient can put the information.
- Provide a procedure for the receiving party to challenge the confidentiality designation.
- Provide a procedure for allowing the producing party to obtain the court's permission to have any such material that will become part of the court record filed under seal. Parties cannot file documents in court under seal by stipulation alone [*Cal Rules Ct, Rule 2.551(a)*].



Strategic Point:

Some trade secret information may be so critical to the success of an enterprise (for example, the secret formula for Coca-Cola), that even when the parties have entered into a stipulated protective order, counsel should promptly make a motion for a protective order that the information need not be disclosed at all. [*See CCP § 2031.060(b)(1), (5)*].



Cross Reference:

Discussion of stipulated protective orders, see *Ch. 9, Gathering and Producing Electronically Stored Information, 9.18*.

Form, San Mateo County Superior Court Model Stipulation and Protective Order Regarding Confidential Information (Single Level of Confidentiality), 9.71.

5.19[8] Counsel Should Discuss How Cost of Production Will Be Allocated Among Parties. The parties are encouraged to discuss how the cost of production of ESI is to be allocated among the parties [*Cal Rules Ct., Rule 3.724(8)(G)*]. As with discovery in general, the presumption is that a responding party will bear the costs of producing electronically stored information. However, the court has the power to shift or apportion the cost of production of electronically stored information [*see CCP § 2031.060(e)*]. Furthermore, if a data compilation must be translated with detection devices, the Electronic Discovery Act provides for shifting of the reasonable costs to the demanding party [*CCP §§ 1985.8(g), 2031.280; Toshiba America Electronics Components v. Superior Court (2004) 124 CA4th 762, 21 CR3d 532*].

Cost-shifting issues arise most often in discovery of electronically stored information that is not reasonably accessible [*see CCP § 2031.060(c)-(e)*]. A party may object to a discovery request on grounds of undue burden or expense because it is from a source that is not reasonably accessible [*see CCP § 2031.210(d)*]. The court may nevertheless order production of information that is not reasonably accessible, and in doing so, may set conditions for the discovery, including allocation of the expense of discovery [*see CCP § 2031.060(e)*].

Consider:

Information not reasonably accessible may include backup tapes, residual deleted matter, and legacy data from a computer system a party no longer uses.

If the parties anticipate discovery of electronically stored information from a source that is not reasonably accessible, they should discuss projected costs of such discovery, as well as possible allocation of the costs among the parties.

When it is necessary to translate data compilations into a reasonably usable form, the "reasonable expense" of the translation shifts to the demanding party [*CCP § 2031.280(e); see Toshiba America Electronics Components v. Superior Court (2004) 124 CA4th 762, 21 CR3d 532*].

 Cross Reference:

Discussion of accessibility and cost shifting, see *Ch. 4, Planning E-Discovery, 4.08[4]*.

5.19[9] Counsel Should Adopt and Document Proposed Discovery Plan. *Cal Rules Ct, Rule 3.724* also requires the parties to consider any other issue relating to the discovery of electronically stored information, including developing a proposed plan relating to the discovery of the information [*Cal Rules Ct, Rule 3.724(8)(H)*].

The parties should consider documenting their agreements on how, and in what format, the parties will produce their ESI. A well-drafted ESI protocol eliminates miscommunication and ensures that all of the parties have the same understanding of whether files will be produced in native, TIFF, or PDF format, what metadata will be included, how confidentiality endorsements will be made, what will be the structure of any load files accompanying the document images, redaction techniques, and production media.

 Cross Reference:

Form, ESI Production Protocol, see 5.31

5.19[10] If Opposing Counsel Is Not Forthcoming, Counsel Should Consider Propounding Interrogatories or Noticing a Deposition. Opposing counsel may not be as cooperative as the Rules of Court require. If opposing counsel is uncooperative, or, more likely, not adequately informed, counsel should consider propounding specially prepared interrogatories or noticing depositions to get the answers that counsel needs in order to proceed with e-discovery.

**Warning:**

Each party is limited to 35 specially prepared interrogatories unless counsel for party propounding the interrogatories signs a declaration explaining why more are required [*see CCP § 2030.050* (requirements for the wording of the declaration)]. Propounding more than 35 interrogatories may invite opposing counsel to move for a protective order, and result in a distracting fight about a topic that is not central to the main issues in the case.

An alternative to propounding interrogatories about the other party's data systems is to depose the opposing party's information technology personnel and/or a corporate designee most knowledgeable about the electronic systems [*see CCP 2025.210*].

 Cross References:

Counsel's ethical obligations in connection with e-discovery, see *Ch. 3, Ethical Issues for Attorneys in E-Discovery*.

Sanctions for delay or lack of cooperation, see *Ch. 13, Seeking or Opposing Sanctions*.

Form, Interrogatories Regarding Electronically Stored Information, see 5.29.



169 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

IV. MEETING AND CONFERRING REGARDING E-DISCOVERY

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.20

AUTHOR: Ernst Halperin, Practice Consultant

5.20 Counsel Should Identify Areas of Agreement and Disagreement.

5.20[1] Counsel Should Determine Which Issues Parties Can Agree On. Determine which issues the parties can agree on, and incorporate any consensus into a discovery plan for production of electronically stored information. This discovery plan should then be incorporated into any case management order established by the court at the initial case management conference [*see Cal Rules Ct, Rule 3.728* (case management order); *see also* 5.25].

5.20[2] Counsel Should Consider Whether Court Intervention May Be Necessary for Unresolved Issues. If consensus cannot be reached, those issues upon which the parties cannot agree should be identified for the court in the case management statement submitted by the parties prior to the initial case management conference.

Paragraph 17(d) of the mandatory Judicial Counsel Form CM-110 Case Management Statement asks the parties to specify anticipated discovery issues for the court.

Cross Reference:

Detailed discussion of case management statements, see Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure, Ch. 23, Case Management.



170 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

IV. MEETING AND CONFERRING REGARDING E-DISCOVERY

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.21

AUTHOR: Ernst Halperin, Practice Consultant

5.21 Counsel Should Prepare and Execute Any Formal Agreements Negotiated at Conference.

After the e-discovery meet and confer conference, counsel should prepare the following documents, as appropriate:

- Discovery plan, including any issues relating to the discovery of electronically stored information on which the parties agree.
- Stipulated order relating to the methods for asserting or preserving claims of privilege or attorney work product.
- Stipulated protective orders regarding confidential information.
- Stipulated ESI production protocol.
- Judicial Counsel Form CM-110 Case Management Statement.



Cross References:

Form of ESI production protocol, see 5.31.

Illustration of Form CM-110, see *Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure*, Ch. 23, *Case Management*, 23.58.

Detailed discussion of case management conferences, see *Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure*, Ch. 23, *Case Management*.

Counsel should consider asking the court to incorporate any agreements reached at the e-discovery conference into the case management order [see 5.25].



171 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

V. ATTENDING CASE MANAGEMENT CONFERENCE

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.22

AUTHOR: Ernst Halperin, Practice Consultant

5.22 CHECKLIST: Attending Case Management Conference.

- ☐ Comply with meet and confer requirements for discussion of issues to be included in initial case management order.

Authority:

Cal Rules Ct, Rule 3.724

Discussion:

See 5.14-5.21

- ☐ Prepare for initial case management conference by integrating any plan for discovery of electronically stored information with general discovery plan to be presented to court at initial case management conference.

Discussion:

See 5.21, 523

- ☐ Attend initial case management conference if required.

Authority:

Cal Rules Ct, Rule 3.722(c), (d)

Discussion:

See 5.23[3]

- ☐ Ask the court to include, in initial case management order, any agreements between parties

concerning discovery of electronically stored information.

Authority:

Cal Rules Ct, Rule 3.728(13)

Discussion:

See 5.25



172 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

V. ATTENDING CASE MANAGEMENT CONFERENCE

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.23

AUTHOR: Ernst Halperin, Practice Consultant

5.23 Options and Strategy Regarding E-Discovery Issues at Case Management Conference.

The ultimate goal for initial procedures in e-discovery is to include in a case management order any agreements or consensus between the parties on issues related to the discovery of electronically stored information.

In addition to the e-discovery meet and confer requirement [see 5.14-5.21], the parties are required to meet and confer to consider other issues commonly included in a case management order [see *Cal Rules Ct, Rule 3.724*].

After both meet and confer requirements have been met, counsel should integrate the resolution of e-discovery issues with the general plan for discovery, which will be considered by the court at the initial case management conference. Counsel should consider presenting any agreements between the parties concerning the discovery of electronically stored information at the case management conference, and asking the court to include such agreements in the case management order.

Cross References:

Meet and confer requirements in non-ESI context, see Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure, Ch. 23, Case Management.

Detailed discussion of case management conferences, see Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure, Ch. 23, Case Management.



173 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

V. ATTENDING CASE MANAGEMENT CONFERENCE

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.24

AUTHOR: Ernst Halperin, Practice Consultant

5.24 Counsel Must Attend Initial Case Management Conference.

5.24[1] Court Must Set Initial Case Management Conference. The court must set an initial case management conference to review the case. In many courts the date of the initial case management conference is set at the time the summons is issued. At the conference, the court will decide whether to assign the case to an alternative dispute resolution process, whether to set the case for trial, and whether to take action regarding matters identified in *Rules 3.727 and 3.728 of the California Rules of Court* [*Cal Rules Ct, Rule 3.722(a)*].

One of those matters identified in the rules is the discovery of electronically stored information. Specifically, the case management order may include "any additional orders that may be appropriate, including orders on matters listed in rules 3.724 and 3.727" [*Cal Rules Ct., Rule 3.728(13)*].

➤ Cross Reference:

Detailed discussion of case management conferences, see *Matthew Bender Practice Guide: California Pretrial Civil Procedure, Ch. 23, Case Management, 23.0623.13*.

5.24[2] Meet and Confer Identifies Issues for Case Management Conference. The meet and confer conferences [see 5.14-5.21] are intended to prepare the parties for the case management conference. If the meet and confer process was conducted in good faith and in accordance with the rules of court, counsel should have identified points of agreement and disagreement regarding the case, including the e-discovery component [see *Cal Rules Ct, Rules 3.724, 3.727* (issues to be discussed by parties)]. Points of agreement and issues should have been reduced to writing [see 5.21], thereby providing a road map for the issues that will need to be discussed at the conference.

5.24[3] Counsel Must Attend Initial Case Management Conference If Required. Counsel for each party and each self-represented party are generally required to appear by telephone or personally at the initial case management conference [*Cal Rules Ct, Rule 3.722(c)*]. However, the court may notify the parties that no appearance is required if, based on its review of the written submissions of the parties and other available information, the court determines that appearances at the conference are not required [*Cal Rules Ct, Rule 3.722(d)*].

If a conference is held, counsel should be prepared to discuss and commit to the party's positions on the issues listed in Rules 3.724 and 3.727 [*Cal Rules Ct, Rule 3.722(c)*]. These include issues relating to the discovery of electronically stored information [*see Cal Rules Ct, Rule 3.724(8)*].

**Strategic Point--Personal Attendance:**

If possible, counsel should try to attend the initial status conference in person. This is especially important if the case has been assigned to a single judge. Some counties operate on a single-assignment system, and even in other counties, complex cases are often single-assigned to a complex litigation department. The initial status conference is counsel's first chance to get to know the person who will be deciding critical issues in the case, and an invaluable opportunity to observe the judge's working style and demeanor.

**Cross Reference:**

Detailed discussion of case management conferences, see *Matthew Bender Practice Guide: California Pretrial Civil Procedure, Ch. 23, Case Management, 23.0623.13*.



174 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference

V. ATTENDING CASE MANAGEMENT CONFERENCE

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.25

AUTHOR: Ernst Halperin, Practice Consultant

5.25 Counsel Must Determine What Orders Should Be Entered Relating to Discovery of Electronically Stored Information.

5.25[1] Court Must Enter Case Management Order. The court must enter a case management order setting a schedule for subsequent proceedings, and otherwise providing for the management of the case [*Cal Rules Ct, Rule 3.728*]. The order may include appropriate orders and other provisions relating to the discovery of electronically stored information [*see Cal Rules Ct, Rule 3.728(13); see also Cal Rules Ct., Rule 3.724(8)*].

5.25[2] Any Agreements Reached by Parties at Meet and Confer Should Be Incorporated Into Case Management and Other Orders. Counsel should request that the court incorporate any agreements reached at the e-discovery conference into the case management order, or into separate orders issued at the same time by the court. This will facilitate later supervision of discovery schedules by the court, and will make the court available to enforce any discovery agreements should disputes arise.

Orders that the parties may want to consider asking the court to enter include:

- Stipulated ESI production protocol [*see 5.18[2]*].
- Stipulated order relating to the methods for asserting or preserving claims of privilege or attorney work product [*see 5.18[5]*].
- Stipulated protective orders regarding confidential information.



175 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference
VI. FORMS

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.26

AUTHOR: Ernst Halperin, Practice Consultant

5.26 Sample Document Preservation Memorandum (Litigation Hold).

Sample Document Preservation Memorandum (Litigation Hold).

From: Legal Department, Mary Jones Enterprises, Inc.

Sent: [date]

Subject: Retention of Documents and Electronic Information During Pendency of Lawsuit (ATTORNEY-CLIENT COMMUNICATION)

ATTORNEY-CLIENT COMMUNICATION--COMPANY CONFIDENTIAL

THIS IS AN URGENT INSTRUCTION FOR YOU TO PRESERVE ALL INFORMATION OF ANY TYPE, HARD COPY OR ELECTRONIC, RELATED IN ANY WAY TO _____ [specify information which needs to be preserved, e.g. THE BUSINESS RELATIONSHIP BETWEEN MARY JONES ENTERPRISES, INC. AND JOHN SMITH]. PLEASE READ THE FOLLOWING INSTRUCTIONS CAREFULLY.

As you may be aware, our company is a _____ [specify plaintiff or defendant] in a lawsuit against _____ [opponent, e.g., John Smith]. The lawsuit contends that _____ [short description of the dispute].

In order to ensure that our company can best prepare its case and meet all of its discovery obligations in connection with this lawsuit, we require that you, and those who report to you, preserve all documents and data that may be relevant to the lawsuit.

Although we have always taken seriously our obligation to secure and produce documents and data that relate to pending litigation, recently there have been a number of courts that have imposed significant penalties on companies who, although they were aware of the claims, did not preserve potentially relevant information. In those cases, along with monetary penalties, the courts assumed that the "missing" documents or data had information that was damaging to the company, simply because the documents or data were not saved when the company knew a lawsuit was threatened.

It is therefore essential that all identified documents and data be retained. To avoid any question as to whether we, or any of our employees, took reasonable steps to secure relevant information, we must require that you save all relevant documents and data currently in your possession, as well as those documents and data found in the future as the result of a good-faith, diligent search effort. To conduct such a search, it is essential that you review your records to see if you have any information that might be responsive to the list of "Potentially Relevant Information" below. It is also essential that managers and supervisors in your work group or organization save all responsive documents as well.

Please follow all instructions in this memorandum closely.

I. WE REQUIRE THAT YOU LOCATE AND PRESERVE ALL POTENTIALLY RELEVANT INFORMATION

Effective immediately, our company is required to preserve all information potentially relevant to this matter, including all memoranda, correspondence, drafts, handwritten notes, telephone messages, charts, data, analyses, tape recordings, text files (Word, Excel, PowerPoint), floppy discs, Zip discs, CD-ROMs, files maintained on a computer hard drive, on-line data compilations, e-mail, calendar entries, logs and data (including code).

As such, do not delete, destroy, discard, alter or otherwise dispose of any such information that relates in any way to this dispute. Furthermore, you must stop all manual and automatic "janitorial" functions such as document purge cycles that affect relevant documents and data, until further notice.

Any question you have as to the relevance of particular information should be resolved in favor of preservation and retention. "Potentially Relevant Information" is to be defined broadly, and includes, but is not limited to:

A. RECORDS RELEVANT TO:

[specify categories of records]

1. _____ *[specify category of potentially relevant information, tracking the language used in the opponent's document requests].*
2. _____ *[specify category of potentially relevant information, tracking the language used in the opponent's document requests].*

B. RECORDS RELATED TO COMMUNICATIONS WITH _____ *[opponent, e.g., JOHN SMITH];*

1. All documents related to any communication with _____ *[opponent, e.g., JOHN SMITH]* regarding _____ *[subject].*
2. All documents related to any communications with _____ *[opponent, e.g., JOHN SMITH]* regarding _____ *[subject].*

II. IN ADDITION TO HARD COPIES, WE REQUIRE THAT YOU PRESERVE AND RETAIN ALL POTENTIALLY RELEVANT INFORMATION STORED ON YOUR INDIVIDUAL HARD DRIVE

We require you to preserve and retain all potentially relevant information, including files and e-mail stored on your individual hard drive. Please follow these instructions carefully.

A. REMOTE COLLECTION (if applicable)

If you are operating on a Windows workstation, such data from your "Documents and Settings" folder can be collected remotely by our company's legal department if you are currently running the connected backup software.

If you are not currently running the connected backup software, please follow these instructions to install and run the program:

Go to the Start menu on your computer, go to Programs, then go to Connected, and then click on Connected to install and run the software. If Connected is not loaded on your computer or if you have questions about installation, please contact the information technology department at 555-555-5555.

If, for any reason, you cannot run the backup software or you believe that all data relevant to the litigation will not be captured in a backup of your "Documents and Settings," please contact IT at IT@company.com.

III. INSTRUCTIONS REGARDING PRESERVATION AND TRANSMISSION OF POTENTIALLY RELEVANT INFORMATION

With regards to the above-listed potentially relevant information, please carefully follow these instructions:

A. PRESERVATION

1. It is critical that the information you preserve is complete and accurate.
2. Personnel in your department (including Human Resources, Payroll, and Legal) must preserve all files where responsive documents reasonably can be expected to be found, including any files that have been sent to storage or to other record custodians, or any files kept by you or your assistant.
3. We specifically emphasize that you are required to preserve all Electronically Stored Information, such as, for example, information stored on computer hard drives, internal or external, backup tapes and metadata, that is reasonably accessible to you.
4. If you have any doubt about whether a record falls within a category on the above list of potentially relevant information, include the record in the documents you preserve.
6. Any record that may be responsive to the list of potentially relevant information should be reviewed to determine whether all attachments referenced in the record are attached. If attachments that are referenced in the record are not attached, efforts should be made to locate and include the attachments with the record. However, under those circumstances, because the referenced attachments were not originally attached to the main record in your files, such attachments should be placed behind, but not attached to, the main record.
7. Any potentially relevant information, including any file folders and labels, where appropriate, should be preserved as they currently exist.
8. Do not create any records that are not presently in existence in response to this request. Right now, you must simply preserve all responsive documents that have already been created.
9. Do not make notes on or otherwise write on any of the documents that you locate.
10. All responsive hard copy documents and files should be put into a folder and/or box. The folder and/or box should

have a cover sheet with the following information:

- a. The name and work telephone number of the individual principally responsible for gathering documents.
- b. The legend: "Privileged and Confidential: Subject to the Attorney-Client Privilege and Work Product Doctrine: Documents Gathered at Counsel's Request."
- c. Any remarks or explanations that may be appropriate.

11. Under no circumstances should you alter or destroy ANY record, document, or file that may be responsive to this memorandum.

We will let you know when the case is over and you can go back to your normal practices with regard to retaining/discarding documents and data in accordance with our company policies.

If you know of anyone else within our company who may be in possession of materials relevant to this matter, please immediately contact _____ [*name and e-mail of in-house counsel contact*].

IV. COMMUNICATIONS REGARDING THE LITIGATION

Please do not speak to any non-company personnel, and specifically any person representing or affiliated with Opponent, regarding this lawsuit or our request that you preserve potentially relevant documents and data. In addition, if you are contacted by anyone not affiliated with our company related to this litigation, please let _____ [*name and e-mail of in-house counsel contact*] know immediately.

In addition to preserving records, you may be asked to provide additional assistance to our company's legal department and/or our company's outside counsel. Any communications between you and our company's lawyers and/or outside counsel for the purpose of providing legal advice or assistance to our company are attorney-client communications related to this litigation matter and, as such, are privileged and confidential. Please do not disclose those communications to anyone.

We are not asking you to create any new documents for purposes of this litigation. If you are subsequently asked by our company's lawyers to create materials or otherwise communicate with them regarding this litigation, please clearly mark such materials and communications "Attorney-Client Communication" and address them only to the appropriate person at our company's legal department or outside counsel.

V. ADDITIONAL COMPANY REPRESENTATIVES WHO MAY HAVE POTENTIALLY RELEVANT DOCUMENTS

If you are aware of anyone else who is not listed as a recipient on this memorandum whom you believe has documents relevant to the dispute, or communications with _____ [*opponent, e.g., JOHN SMITH*] regarding the dispute, please contact _____ [*name and e-mail of in-house counsel contact*].

VI. CONCLUSION

We apologize in advance for any disruption this Directive causes in the regular performance of your duties. Our company recognizes the burden of this request, and truly appreciates your understanding and patience during this process.

Thank you for your attention and cooperation in this matter.

Legal Department, MARY JONES ENTERPRISES, INC.

VII. CONFIRMATION OF RECEIPT AND REVIEW OF THIS DIRECTIVE

Please read the following statement, and indicate your assent by replying to this e-mail to directive@company.com

"I have read this Directive and understand that I should preserve the listed types of documents and data. I also understand that, if I have any question regarding the types of documents and data that I am required to preserve or any related question I should contact [_____ *name and e-mail of in-house counsel contact*]."

NOTES:

Advising Client of Duty to Preserve:

See 5.06



Related Form for Preservation Demand to Opposing Party:

See 4.17



176 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference
VI. FORMS

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.27

AUTHOR: Ernst Halperin, Practice Consultant

5.27 Client ESI Interview Checklist.

Client Interview-ESI Discovery Response Questions E-Mail, E-File and System Backups

☐ Document retention programs/practices:

☐ Does client have a written document retention program? If yes, does the program have the following items in writing?

☐ A document retention policy.

☐ A document retention schedule or other document that identifies custodians or persons responsible for carrying out archival and destruction functions?

☐ Has the retention program changed during the relevant time frame? *[Obtain copies of retention program documents that pertain to the relevant time period. If the policy has changed during the relevant time period, obtain the applicable outdated versions as well.]*

☐ If there is not official retention program, are there retention/destruction/backup practices for affected custodians, departments, the corporate IT group in general?

☐ For each practice, who is the person most knowledgeable who can talk to you about what was done for archiving, retention, and destruction of ESI during the relevant time period?

☐ Has client taken any steps to identify ESI relevant to the instant litigation, and to halt destruction or

collect the ESI?

- ☐ If no, work with client to institute a reasonable and defensible litigation hold as soon as possible.
- ☐ If yes:
- ☐ What steps were taken to identify relevant ESI?
 - ☐ Is there documentation of the steps taken and persons notified and/or talked to?
- ☐ What steps were taken to halt destruction?
- ☐ Is there documentation of the steps taken and persons notified and/or talked to?
- ☐ If ESI has been collected, what collection personnel and methods were used?
- ☐ Personnel: name, whether in-house or outside vendor, title/function, forensic collection qualifications (forensic collection certifications such as EnCe, CISSP, etc.) and essential details of experience in forensic collections.
 - ☐ Methods: What collection tools were used? (Are they recognized in the legal industry as forensically sound, i.e., capable of creating a reliable, forensic quality, bit for bit copy? "Drag and drop" methods do not meet these criteria.)

[The two general sources to speak with personally are "key players" and corporate IT personnel. Key players are those persons who are likely to have relevant information regarding the litigation matter (Zubulake v. UBS Warburg LLC (SDNY 2003) 220 FRD 212, 218) . Key Players will know about the kind of ESI created by individuals. Zubulake v. UBS Warburg states that counsel should make every attempt to speak personally with key players (Zubulake v. UBS Warburg LLC (SDNY 2003) 220 FRD 212, 218) .

Corporate IT will know about the kinds of information that is created by or maintained by the corporation itself--HR databases, corporate e-mail servers, backup media, etc. *Corporate IT will also know something about the data creation habits of the individual Key Players. Check any information obtained from key players with Corporate IT.]*

☐ Key players:

☐ Who are the "key players" currently known to client? Start with:

- ☐ Persons involved in the subject matter.
- ☐ Employees identified in the complaint (name or title or function).
- ☐ Assistants and other ESI custodians who work with the two categories above.

- ☐ When speaking with key players, ask who else might have relevant ESI.
- ☐ For each key player, identify all ESI creation and storage devices to which client has right of access:
 - ☐ Laptops.
 - ☐ Office workstation.
 - ☐ Home office workstation.
 - ☐ Does person perform work on home computers?
 - ☐ Guest office workstations.
 - ☐ PDAs/cell phones.
 - ☐ iPod/other MP3 and data storage devices.
 - ☐ Removable storage media--floppy discs, thumb drives, CD-ROMs, removable hard drives, etc.
- ☐ For device identified, has key player changed devices during the relevant time frame?
 - ☐ Has person been issued a new laptop, PDA, etc.?
 - ☐ If yes, what happened to the old machine?
- ☐ For each device identified, has the device ever been backed up?
 - ☐ By corporate IT or by the key player, or both?
 - ☐ If key player backs up the device, where are all backups located?
 - ☐ If key player backs up the device:
 - ☐ Inform key player that all backups from the relevant time period cannot be altered or deleted, and must be preserved for the pending litigation.
 - ☐ If a litigation hold notice has not already been sent to this key player, follow up immediately with written confirmation of notice of need to preserve.

☐ Does key player store information on the corporate network?

☐ If yes, where?

☐ If key player's laptop computer were to crash, or be destroyed by an earthquake, would all of the information on the laptop be lost?

☐ If not, where would key player go to retrieve information?

[Check on all of the information received from the key players. Is the device list accurate? Replacement machine details? Backups?]

☐ Corporate IT personnel:

☐ For each key player:

☐ What access does their login give them on the corporate network?

☐ Where is their data stored on the network (private network shares, or other locations)?

☐ E-mail:

☐ System history:

☐ What is the current enterprise e-mail system in use (Exchange, Notes/Domino, Groupwise, etc.)?

☐ What version is currently in place?

☐ How long has this system been in use?

☐ What is the system architecture?

☐ How many servers are currently in use?

☐ How many sites are currently in the enterprise?

☐ How are these sites connected (SMTP, POP, Native Protocols)?

☐ Are there offline capabilities for traveling users/laptops?

☐ Was there a prior system?

☐ What was the prior system?

☐ When was it officially retired from service?

☐ Was the system migrated and data converted to the new system?

☐ Are backups or data files from the old system still available?

☐ General:

☐ Are there size restrictions on server mailboxes?

☐ What are the restrictions?

☐ Are there exceptions?

☐ Are users able to and/or trained on how to create local drive stores for their e-mail?

☐ Is there an archiving policy in place?

☐ If so, what is it?

☐ Is it automated or manual?

☐ Do users keep mail stores on shared network drives as well as local drives?

☐ Can users forward their e-mail to external accounts?

☐ Are users issued Blackberries or other PDAs with corporate e-mail connectivity?

☐ E-files:

☐ System history:

☐ What network operating system(s) are in place (Netware, Windows, UNIX/LINUX, etc.)?

- ☐ How long have these systems been in place?
- ☐ Were they preceded by a prior system?
 - ☐ What was the prior system?
 - ☐ When was it officially retired from service?
 - ☐ Was the system migrated and data converted to the new system?
 - ☐ Are backups or data files from the old system still available?
- ☐ Are any processes for archiving or data migration to off-line storage in place?
- ☐ Do users have access to a corporate FTP site for file transfers?
 - ☐ Is access restricted or is there a general login provided for all users?
 - ☐ Is this data backed up along with other network resources?
- ☐ General
 - ☐ Is there an enterprise document storage policy?
 - ☐ What is it?
 - ☐ Are any document management systems in place (i.e. MS SharePoint, IBM/Lotus QuickPlace)?
 - ☐ Are these used on a regular basis?
 - ☐ Are there retention and revision controls in place?
 - ☐ Are these systems included in the enterprise backup plan?
 - ☐ Is security and administration centralized or distributed (i.e., enterprise domain vs. local domains vs. workgroups)?
 - ☐ Common configurations:
 - ☐ Is there a standard corporate PC configuration?

- ☐ What is it?
- ☐ What systems are in place (Dell, IBM, HP)?
- ☐ Common HD sizes?
- ☐ Are there any non-PC based systems in place (AS/400, Apple, mainframe, proprietary systems)?
- ☐ What common OS is in place on users local machines?
 - ☐ OS (Windows, Linux, OS/2).
 - ☐ Version (XP Pro, XP Home, 2000 Pro, 98, 95).
- ☐ File system (NTFS, FAT32, FAT16).
- ☐ Percentage of client organization for each type of configuration.
- ☐ Is there any file encryption technology in place on users' machines?
 - ☐ Full Drive, Windows EFS, PGP?
 - ☐ Does corporate IT have access to de-crypt files without users' knowledge/cooperation?
- ☐ Are users provided with a network drive share for private use (home drive)?
 - ☐ How do these map to servers and physical drives?
 - ☐ Are there space restrictions enforced on the home drives?
 - ☐ Are there exceptions to these restrictions?
- ☐ Are users provided with common network drive shares for group use?
 - ☐ What are they?
 - ☐ How do they map to servers and physical drives (i.e., P: maps to the SHARE PROJECT directory of local drive D: on server W2_FILE01)?

☐ Storage:

☐ Are user documents stored on shared network drives and/or local drives?

☐ Is there a general tendency towards one location or the other?

☐ Are users able and/or permitted to use USB ThumbDrives, PDAs, iPods and other removable storage media in conjunction with corporate PCs?

☐ Are the cables and/or cradles available to synchronize them with a computer?

☐ What brands and models?

☐ Do they have removable memory cards?

☐ Backup:☐ General:

☐ Is there an enterprise backup policy?

☐ Is it documented?

☐ Can a copy be provided?

☐ Are backups taken on a scheduled basis?

☐ How often are full backups taken?

☐ How often are differential backups taken?

☐ How long are backups retained?

☐ Do backups differ for e-mail and e-file systems?

☐ How?

☐ What is the backup architecture?

☐ Are backups periodically verified for accuracy and restorability?

- ☐ How often?
- ☐ When was this last done?
- ☐ Is the purpose of the backup for disaster recovery, data retention, or both?
 - ☐ What backup software (brand and version) is in use?
 - ☐ Is the backup centralized or distributed?
 - ☐ If distributed, how many sites?
 - ☐ Do all sites use the same software and hardware?
- ☐ Are backups stored locally on-site, centrally on-site, off-site or a combination?
 - ☐ What is the policy for tape storage (local, central, and off-site)?
 - ☐ Are tapes on a rotation (explain)?
- ☐ What type and size of media are the backups written to (DLT, LTO, multiple, etc)?
- ☐ E-mail:
 - ☐ For what time period do backups of the e-mail system currently exist?
 - ☐ Are any backups in this time period known to have failed?
- ☐ E-file:
 - ☐ For what time period do backups of network shared resources currently exist?
 - ☐ Are any backups in this period known to have failed?
 - ☐ Are (none/some/all) user local drives backed up?
 - ☐ Is the backup centralized or user controlled?
 - ☐ Is this an automated process?

☐ What is the primary backup media (USB Drive, Tape, ZIP, JAZ, Network Share)?

NOTES:

Source of Form:

Form prepared by Diane E. Barry, Esq., Director of Discovery Strategy & Management, International Litigation Services, Inc.

Discussion:

See 5.06[4]



177 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference
VI. FORMS

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.28

AUTHOR: Ernst Halperin, Practice Consultant

5.28 Demand Letter with Document Preservation Demand.

Demand Letter with Document Preservation Demand.

[date]

TO: Mary Jones Enterprises, Inc.
Attention: Jane Lee, General Counsel
100 North Main St., Suite 200
Farallon City, California 90000

Dear Ms. Lee:

Please be advised that our client, John Smith, is involved in a dispute against Mary Jones Enterprises, Inc., arising out of _____ [describe dispute in detail, including background, factual basis, and current status of dispute].

Our client, John Smith, hereby requests that Mary Jones Enterprises immediately take the following measures to resolve the dispute with John Smith: _____ [describe in detail the relief being requested, including any payment of damages and any other actions that the prospective defendant would have to perform to satisfy the prospective plaintiff].

DEMAND FOR PRESERVATION OF EVIDENCE

Please be further advised that we believe that electronically stored information ("ESI") is an important and irreplaceable source of discovery and/or evidence in connection with the dispute described above. If litigation is necessary to protect Mr. Smith's rights, the discovery requests to be served in this matter will seek information from computer systems, removable electronic media and other locations for Mary Jones Enterprises, Inc., as well as from any agents and individual employees of Mary Jones Enterprises, Inc., who were involved in or dealt with matters relevant to the dispute

described above. This includes, but is not limited to, e-mail, instant messaging, text messages, voice mail messages, and other electronic communications, word processing documents, spreadsheets, databases, calendars, telephone logs.

Therefore, YOU ARE HEREBY GIVEN NOTICE to immediately take all steps necessary to prevent the destruction, loss, concealment, or alteration of any paper, document, or electronically stored information and other data or information generated by and/or stored on your computers and storage media (e.g., hard disks, floppy disks, backup tapes, etc.), and e-mail related to _____ [*subject matter of lawsuit*].

ESI should be afforded the broadest possible definition and includes, but is not limited to, all digital communications (e.g., e-mail, voice mail, instant messaging), word processed documents (e.g. Word and WordPerfect documents and drafts), spreadsheets and tables (e.g. Excel and Lotus 123 worksheets), accounting application data (such as QuickBooks, Money, or Peachtree), image and facsimile files (including PDF, TIFF, JPG, and GIF images), sound recordings (including WAV and MP3 files), video recordings, all databases, all contact and relationship management data, calendar and diary application data, online access data (including temporary, Internet files, History, and Cookies), all presentations (including PowerPoint and Corel), all network access and server activity logs, all data created with the use of any Personal Data Assistant (PDA) such as Palm Pilot, Blackberry, or other Windows-based or Pocket PC devices, all CAD files, and all back-up and archival files.

Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. You must also intervene to prevent loss due to routine operations and employ proper techniques to safeguard all such evidence.

Because hard copies do not preserve electronic searchability or metadata, they are not an adequate substitute for ESI. If information exists in both electronic and paper form, you should preserve them both.

Litigation Hold

You are requested to immediately initiate a litigation hold for potentially relevant ESI, documents, and tangible things, and to act diligently and in good faith to secure and audit compliance with that litigation hold. You are also requested to preserve and not destroy all passwords, decryption procedures (including, if necessary, the software to decrypt the files), network access codes, ID names, manuals, tutorials, written instructions, decompression or reconstruction software, and any and all other information and things necessary to access, view, and (if necessary) reconstruct any ESI. You should not pack, compress, purge, or dispose of any file or any part thereof.

You are further requested to immediately identify and modify or suspend features of your operations, information systems, and devices that, in routine operations, operate to cause the loss of documents, tangible items, or ESI. Examples of such features and operations include, but are not limited to, purging the contents of e-mail repositories by age, capacity, or other criteria; using data or media wiping, disposal, erasure, or encryption utilities or devices; overwriting, erasing, destroying, or discarding backup media; reassigning, re-imaging or disposing of systems, servers, devices, or media; running antivirus or other programs that alter metadata; using metadata stripper utilities; and destroying documents or any ESI by age or other criteria.

Servers

With respect to servers like those used to manage electronic mail and network storage, the entire contents of each user's network share and e-mail account should be preserved and not modified.

Storage

With respect to on-line storage and/or direct access storage devices attached to your mainframe computers and/or minicomputers, in addition to the above, you are not to modify or delete any ESI, "deleted" files, and/or file fragments existing on the date of this letter's delivery that contain potentially relevant information.

With regard to all electronic media used for off-line storage, including magnetic tapes and cartridges, optical media, electronic media, and other media or combinations of media containing potentially relevant information, you are requested to stop any activity which may result in the loss of any ESI, including rotation, destruction, overwriting and erasure in whole or in part. This request is intended to cover all media used for data or information storage in connection with your computer systems, including magnetic tapes and cartridges, magneto-optical disks, floppy diskettes, and all other media, whether used with personal computers, minicomputers, mainframes or other computers, and whether containing backup and/or archival ESI.

Personal Computers

You should take immediate steps to preserve all ESI on all personal computers used by your officers, directors and employees, including all secretaries and assistants, that in any way relate to _____ [*subject matter of action*]. As to fixed devices, (1) a true and correct copy is to be made of all such ESI, including all active files and completely restored versions of all deleted electronic files and file fragments; (2) full directory listings (including hidden files) for all directories and subdirectories (including hidden directories) on such fixed devices should be written; and (3) all such copies and listings are to be preserved until this litigation is ended. Floppy diskettes, CDs, DVDs, tapes, and other non-fixed media relating to this matter are to be collected and stored pending resolution of this litigation.

Portable Systems

In addition to your immediate preservation of ESI, documents and tangible items in your business, on servers and workstations, you should also determine if any home or portable systems may contain potentially relevant data or information. To the extent that officers, board members, or employees have sent or received potentially relevant e-mails or created or reviewed potentially relevant documents away from the office, you must preserve the contents of systems, devices, and media used for these purposes (including not only potentially relevant data from portable and home computers, but also from portable thumb drives, CD-R discs, PDAs, smart phones, voice mailboxes, or other forms of ESI storage). Additionally, if any employees, officers, or directors used online or browser-based e-mail accounts or services to send or receive potentially relevant messages and attachments, the contents of these account mailboxes should be preserved.

Evidence Created or Acquired in the Future

With regard to documents, tangible things, and ESI that are created or come into your custody, possession, or control subsequent to the date of delivery of this letter, potentially relevant evidence is to be preserved. You should take all appropriate action to avoid destruction of potentially relevant evidence.

Please forward a copy of this letter to all persons and entities possessing or controlling potentially relevant evidence. Your obligation to preserve potentially relevant evidence is required by law.

Please contact Tom Doe, attorney for John Smith, if you have any questions regarding this letter.

[Optional meet and confer]

Sincerely,
Tom Doe
California Bar Number 987654
100 North Main St., Suite 200
Farallon City, California 90000
Phone: 555-555-5555
Attorney for Plaintiff, John Smith

NOTES:

Source of Form:

Reproduced, with modifications, from Keisel & Williams, "California E-Discovery: Analysis of the 2009 Legislation and Rules" (LexisNexis 2009), with acknowledgment to Steve Williams, Cotchett, Pitre & McCarthy, Burlingame, CA

Authority:

Cal Rules Ct, Rule 3.724(8)

Use and Content of Preservation Notice:

See 5.10-5.12



178 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference
VI. FORMS

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.29

AUTHOR: Ernst Halperin, Practice Consultant

5.29 Interrogatories Regarding Electronically Stored Information.

Interrogatories Regarding Electronically Stored Information.

Tom Doe

California Bar Number 987654

100 North Main St., Suite 200

Farallon City, California 90000

Phone: 555-555-5555

Attorney for Plaintiff, John Smith

SUPERIOR COURT OF CALIFORNIA,

COUNTY OF FARALLON

	)	
	)	No. _____
John Smith,	)	FIRST SET OF SPECIALLY PREPARED
Plaintiff, vs. Mary Jones Enterprises, Inc.,	)	INTERROGATORIES OF
Defendant.	)	PLAINTIFF JOHN SMITH TO DEFENDANT
	)	MARY JONES
	)	ENTERPRISES, INC.
	)	

Propounding Party: PLAINTIFF JOHN SMITH

Responding Party: DEFENDANT MARY JONES ENTERPRISES, INC.

Set Number: One

To Defendant, MARY JONES ENTERPRISES, INC. and to JANE LEE, the attorney of record for Defendant:

Plaintiff requests that Defendant answer the following interrogatories separately, fully, and under oath, and serve the answers on Plaintiff within _____ [state period for answer, e.g., 30 days] after the service of these

interrogatories.

[If responding party is a corporation, governmental agency, or other entity, add]

In order to answer these questions, you must select an officer or agent who must answer these questions with all information available to you.

[CONTINUE]

1. State the name and address of all persons who helped you answer these interrogatories, and their relationship to you.
2. IDENTIFY all computers and computer systems currently in use by your company. IDENTIFY, for purposes of this interrogatory means to state the number, types, locations, operating systems, and users associated with each of the computers or computer systems currently in use by you.
4. IDENTIFY all current and former personnel who have or had access to network administrator, backup, archiving, or other system operations, for the period _____ [dates]. IDENTIFY, for purposes of this interrogatory means to state the person's name, title, contact information, and job description or duties.
5. IDENTIFY all data systems that have been used to store, receive, or generate data related to the subject matter of this litigation. For purposes of this interrogatory, IDENTIFY means to state the type of data system, the current location of the data system, generally describe the subject matter of the data on the system, and whether the system is still in use.
6. Describe your policies regarding employee use of company computers and company data systems.
7. IDENTIFY any policy you have for retention and disposition of electronically stored information including retention periods for each kind of electronic data.
8. IDENTIFY any electronically stored information ("ESI") relating to the subject matter of this litigation that may have been deleted. IDENTIFY, for purposes of this interrogatory means to state the subject matter of the ESI, the type or format of the ESI, any document custodian with whom the ESI was associated, the creation date, and the destruction date.
9. IDENTIFY your backup systems for electronically stored information ("ESI"). For purposes of this interrogatory, IDENTIFY means to describe the backup system, and types of storage media used.
10. Do backup media exist for the period _____ [describe period of time relevant to the lawsuit, e.g., January 2008 through December 2009]?
11. IDENTIFY all backup media that ever contained ESI which may relate to the issues in this litigation from the time periods identified in your response to Interrogatory No. 8, and which have been destroyed or overwritten. For purposes of this interrogatory, IDENTIFY means to describe the medium and the subject matter of its contents, and state the date when it was destroyed or overwritten.
12. IDENTIFY your e-mail system. For purposes of this interrogatory, IDENTIFY means to state the kind of system (for example, Outlook server, Lotus Notes, etc.) and describe the system settings for automatic deletion of e-mails.
13. DESCRIBE all efforts you have made to identify and save electronically stored information that may be relevant to this action.

14. DESCRIBE any electronically stored information pertaining to the subject matter of this lawsuit that you contend is not reasonably accessible. For purposes of this interrogatory, DESCRIBE means to identify the source of the information, the general subject matter of the information, and state the reason it is not reasonably accessible.

15. IDENTIFY all computers or computer systems you have replaced since _____ [date relevant to incident giving rise to lawsuit]. For purposes of this interrogatory, IDENTIFY, for purposes of this interrogatory means to state the number, types, locations, operating systems, and users associated with each of the computers or computer systems.

16. For any computers or computer systems you identified in response to Interrogatory Number 15, IDENTIFY all electronically stored information that has been lost as a result of the computer or computer system replacement. IDENTIFY, for purposes of this interrogatory means to state the subject matter of the ESI, the type or format of the ESI, any document custodian with whom the ESI was associated, the creation date, and the destruction date.

NOTES:

Discussion:

See 5.19[10]



Timing:

See 5.19[10]



179 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference
VI. FORMS

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.30

AUTHOR: Ernst Halperin, Practice Consultant

5.30 "Meet and Confer" Checklist.

"MEET AND CONFER" CHECKLIST

[This checklist is designed to cover the basic ESI production issues required for discussion prior to Case Management Conference under Ca. Rules Ct, Rule 3.724(8). Counsel should be prepared to answer the following questions, and expect to receive detailed information on the same subjects from all opposing parties.]

☐ Scope of discovery, including ESI discovery [Cal Rules Ct, Rule 3.273(8)(D)].

[For this category, counsel should prepare at least two lists ahead of time: one regarding the key players for the client, and one regarding the key players counsel is aware of for each opposing party.]

☐ What is the relevant time frame for this litigation?

☐ Who are the relevant "key players" whose ESI must be preserved?

☐ Names.

☐ Titles/functions.

☐ Departments or office locations.

☐ Brief description of involvement (kind of information or ESI that will need to be identified and preserved).

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.30

- ☐ For each such person, what ESI creation and storage devices do they use (laptop, workstations, PDA, cell phone, home work station, etc.)?
- ☐ For each such device:
- ☐ What are the backup procedures for this device?
 - ☐ How long are such backups kept?
 - ☐ For what time period are backups available?
- ☐ What corporate information needs to be preserved?
- ☐ Accounting.
 - ☐ HR.
 - ☐ Sales.
 - ☐ Other.
 - ☐ For each such department:
 - ☐ What kinds of programs does the department work with?
 - ☐ What kinds of ESI do they generate?
 - ☐ How is it stored (current format)?
 - ☐ Where is it stored (in-house on servers, cloud computing on servers in Taiwan, etc.)?
 - ☐ What are the backup or archiving procedures for that data?
 - ☐ For what time period is this data available?
 - ☐ If not covered above, are there any other categories of information which will need to be produced?
- ☐ Is counsel currently aware of any issues that will affect counsel's client's ability to preserve discoverable ESI [Cal

Rules Ct, Rule 3.273(b)(1)]?

- ☐ Are there any legacy systems or legacy storage media to contend with?
 - ☐ Estimate of costs of data retrieval from same?
- ☐ Is there data missing from the relevant time frame, such as:
 - ☐ Computers of persons no longer with the company--computer went with employee or was recycled?
 - ☐ Other employee or corporate computers that have been wiped or otherwise recycled?
 - ☐ Damaged storage or backup media?
 - ☐ Recycled backup or storage media?
 - ☐ Other?

☐ In what format(s) would clients/opposing party like to produce/receive ESI productions [Cal Rules Ct, Rule 3.273(b)(3)]?

- ☐ Will this be a native production?
- ☐ Shared online repository?
- ☐ Data with TIFFs/PDFs?
- ☐ Exchange of databases?
 - ☐ What kind/program?
- ☐ Exchange of database load files?
 - ☐ What kind/program?
- ☐ Other?

☐ Desired production date(s) [Cal Rules Ct, Rule 3.273(b)(3)].

☐ Privilege Issues.

[If stipulation regarding privilege review is desired, bring a proposed stipulation or e-mail one in PDF format; see 5.19[7].]

☐ Is clawback procedure set out in *CCP* § 2031.285 acceptable [Cal Rules Ct, Rule 3.273(b)(5)]?

☐ If not, what clawback procedure would counsel prefer?

☐ How will the parties assert and preserve:

☐ Confidentiality?

☐ Privacy of third parties?

☐ Trade secrets/proprietary information?

☐ How will cost of production of electronically stored information be allocated among the parties [Cal Rules Ct, Rule 3.273(b)(7)]?

☐ General Cost Sharing: If counsel's client would like to share costs--such as imaging, a joint repository, other expenses:

☐ Request cost sharing arrangements.

☐ Provide an estimate of the costs and savings.

☐ Inaccessibility due to undue burden or cost: If counsel is taking the position that any of the desired and otherwise relevant ESI is inaccessible due to undue burden or cost pursuant to *CCP* § 2031.060:

☐ Give opposing counsel notice that other side will be expected to pay for the discovery.

☐ Provide estimate of the costs associated with doing so.

☐ Translation of data compilations: If counsel is taking the position that any of the desired and otherwise relevant ESI must be "translated through use of detection devices" under *CCP* § 2031.280 and *Toshiba v. Superior Court* (2004) 124 CA4th 762, 21 CR3d 532, and therefore must be performed at the reasonable expense of the requesting party:

☐ Give notice.

☐ Provide estimate of costs and an estimate of the costs.

☐ Any other issues relating to discovery of electronically stored information, including developing a proposed discovery plan relating [Cal Rules Ct, Rule 3.273(b)(8)].

NOTES:

Source of Form:

Form prepared by Diane E. Barry, Esq., Director of Discovery Strategy & Management, International Litigation Services, Inc.

Discussion:

See 5.14-5.21.



Timing:

5.17[1].



180 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference
VI. FORMS

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.31

AUTHOR: Ernst Halperin, Practice Consultant

5.31 Sample ESI Production Protocol.

Sample ESI Production Protocol.

ESI PRODUCTION PROTOCOL

1. Obligation to Produce Electronically Stored Information. The parties acknowledge and agree that to the extent they possess electronically stored information ("ESI") responsive to a document request, that ESI is within the scope of matters subject to discovery in this case.

2. Load Files. Except for ESI described in sections 3(b) and (c) below, ESI will be produced in electronic format, with files suitable for loading into a litigation support database. The load files will define document breaks, attachments and other information identified below.

(a) Document Cross-Reference File. The producing party will provide a cross-reference file that identifies the start and end of the document, its attachments and its corresponding metadata.

(b) Cross-Reference or Linking File. The producing party will also provide a cross-reference file that facilitates the linking of the produced image or native file with the litigation database. This cross-reference file will contain fields such as the unique document ID (i.e., BegBates) and the file path of the corresponding image or native file. The producing party may provide this information either in a litigation database format or as a standard delimited ASCII text file.

3. Categories of Production of ESI. ESI will be produced as follows, depending on its classification.

(a) Production of ESI as TIFF Images With Metadata and Extracted Text. Documents created in standard office automation file formats (including but not limited to Microsoft Word or WordPerfect documents) and ESI that can practicably be converted into TIFF format will be produced as single-page TIFF Group IV images, with any available

fielded metadata and text searchable information extracted from the native documents.

(i) **Bates Numbering.** The producing party will brand all TIFF images in the lower right-hand corner with its corresponding Bates number, using a consistent font type and size. The Bates number must not obscure any part of the underlying image.

(ii) **File Names.** Image file names will be identical to the corresponding Bates numbered images, with a ".tif" file extension.

(iii) **Confidentiality Endorsements.** The producing party will brand any confidentiality or similar endorsements in a corner of the TIFF image. Those endorsements must be in a consistent font type and size, and must not obscure any part of the underlying image or Bates number.

(iv) **Production of Extracted Full Text.** The producing party will provide extracted full text (i.e., text extracted from ESI) for all material originating as ESI in a text file corresponding to a single page of a document. The full text file name will be composed of the Bates number of the associated document, with a ".txt" file extension. When a party is unable to produce extracted full text, it will provide an explanation of that inability with its document production.

(v) **Production of Metadata.** The producing party will provide the following metadata, as applicable, for all ESI: start Bates, end Bates, start attachment, end attachment, custodian or source, original file path, original file name, file type/file extension, MD5 hash value, title, creation date, creation time, page count, last modification date, last modification time, and last saved by name.

(vi) **Metadata for E-Mail.** In addition to the metadata to be produced for all ESI, for all e-mail, the producing party will also produce the following as fielded metadata: subject, author, recipients, from, to, copyees, blind copyees, date sent, time sent, date received, time received, MD5 hash value, attachment file name, begin attachment, and end attachment. Family relationships among e-mail and attachments will be maintained by ensuring that attachments immediately follow their parent e-mail, and setting the "begin attachment" and "end attachment" metadata fields appropriately.

(vii) **Explanation of Inability to Produce Metadata.** When a party is unable to produce metadata for a particular field, it will provide an explanation of that inability with its document production.

(viii) **Redaction.** If a file that originates in ESI needs to be redacted before production, the file will be rendered in TIFF, and the TIFF will be redacted and produced. However, to the extent that the text is searchable in the native format, the producing party will still provide searchable text for those portions of the document that have not been redacted.

(b) **Production of Native Format Documents That Are Impractical to Convert to TIFF.** ESI that is not practical to convert to TIFF may be produced using one of the two following methods, which method will be subject to meet and confer between the parties.

(i) **Spreadsheets That Are Impractical to Convert to TIFF.** ESI that is not practical to convert to TIFF (for example, spreadsheets) may be produced in electronic format suitable for loading to a litigation support database with links to the native files.

(A) **Identification.** ESI produced in native file format will be assigned a unique DocID number within the litigation database.

(B) **File Names.** File names will be identical to the DocID number, followed by the original file name and file extension.

(C) **Authentication.** The producing party will provide a litigation database load file with separately fielded data, which will contain, as one of the fields, the MD-5 hash value of each file produced in native format.

(ii) **ESI That Is Impractical to Produce With Links to a Database.** The parties understand and acknowledge that certain categories of ESI are structurally complex and do not lend themselves to production as native format documents with links to a litigation database. For example, in some instances renaming and/or linking a native document comprised of subparts will render the document unusable. After meet and confer, the parties may agree to produce these types of documents in native form, accompanied with a Bates number and MD5 hash value, but separate from a litigation support database. In those instances, if a propounding party or its experts lack access to proprietary software needed to review the producing party's ESI in native format, the parties will meet and confer to obtain a resolution which allows that party to view the affected documents.

(iii) **Encrypted or Password-Protected ESI.** For any ESI that exists in encrypted format or is password-protected, the producing party will provide the propounding party a means to gain access to those native files (for example, by supplying passwords).

(c) **Reports in Lieu of Native Production.** If a party believes that it would be impractical to produce ESI in native format because of complexities associated with certain scheduling programs (such as Primavera), accounting systems, mapping systems, and/or other databases (such as MS Access, Oracle, and Microsoft SQL Server), it will so notify the propounding party and will inform the propounding party whether it has generated reports in the normal course of business using those programs or systems. In any such instance, the parties will meet and confer concerning the manner of production of those reports.

(d) **Production of Pictures/Images.** Any photographic images created and/or maintained in electronic format will be produced in that format.

4. **Production Media.** The producing party will use the appropriate electronic media (CD, DVD or hard drive) for its ESI production, and will cooperate in good faith to use the highest-capacity available media to minimize associated overhead. The producing party will label the physical media with the producing party, production date, media volume name, and document number range.

5. **Avoidance of Duplicate Production.** Each producing party will take all reasonable steps to reduce duplication of ESI. De-duplication will be performed within a custodian. The producing party will maintain references to all removed duplicate files.

Signed and agreed on _____ [date]

_____ [signature of party]

[typed name]

Signed and agreed on _____ [date]

_____ [signature of party]

[typed name]

NOTES:

Source of Form:

Form reproduced from Kiesel & Williams, "California E-Discovery: Analysis of the 2009 Legislation and Rules" (LexisNexis 2009), with acknowledgment to Steve Williams, Cotchett, Pitre & McCarthy, Burlingame, CA

Authority:

Cal Rules Ct, Rule 3.724(8)

Content of Protocol:

See 5.19[9]



181 of 181 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5 Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference
VI. FORMS

1-5 MB Practice Guide: CA E-Discovery and Evidence 5.32

AUTHOR: Ernst Halperin, Practice Consultant

5.32 Sample Letter to Opposing Counsel Regarding Document Preservation Steps Taken.

Sample Letter to Opposing Counsel Regarding Document Preservation Steps Taken.

[date]

Mr. Tom Doe
100 North Main St., Suite 200
Farallon City, California 90000

RE: Smith v. Mary Jones Enterprises, Inc.

Dear Mr. Doe:

This letter confirms our conversation during the meet and confer session held on _____ [date]. Our company has issued a litigation hold memorandum to employees who may have information relevant to the subject matter of this lawsuit. The clearing of data on servers likely to contain custodians' information related to the subject matter of the lawsuit has also been suspended. The company has identified _____ [number, e.g., two] server[s] likely to contain information related to this lawsuit, and the disaster recovery backup tape re-use cycle has been suspended for those servers.

If you believe any of the measures taken are inadequate, please notify me at once.

Sincerely,
Jane Lee
California Bar Number 123456
50 South Main St., Suite 100

Farallon City, California 90000

Phone: 555-999-9999

Attorney for Defendant, Mary Jones Enterprises, Inc.

NOTES:

Contents of letter:

See 5.07[5]



Timing:

See 5.07[5]



1 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.syn

AUTHOR: Diane E. Barry, Esq.

§ 5A.syn Synopsis to Chapter 5A: E-Discovery Deposition Practice

5A.01 Scope.

5A.02 Objective and Strategy.

5A.03 CHECKLIST: Complying With Legal Requirements for Taking a "Person Most Knowledgeable" Deposition

5A.04 Objective and Strategy.

5A.05 CCP § 2025.230 Authorizes Taking Deposition of Organization Rather Than a Specific Natural Person.

5A.06 PMK Deposition Notice Cannot Specify Deposition of a Particular Person.

5A.07 PMK Deposition Notice Must Specify Deposition Topics With "Reasonable Particularity."

5A.08 PMK Deposition Notice Can Request Production of Documents at Deposition.

5A.09 PMK Deposition Notice Must Specify If Testimony Will Be Recorded and If Recording May Be Used at Trial.

5A.10 No Specified Limits on Number of Topics That Can Be Noticed.

5A.11 Place for Taking PMK Deposition.

5A.11[1] Place When Deponent Is a Party.

5A.11[2] Place When Deponent Is Not a Party.

5A.12 Organization Must Identify, Educate, and Produce Person(s) "Most Qualified" to Testify As to All Reasonably Available Corporate Knowledge on Identified Subjects.

5A.12[1] PMKs Need Not Have Actual Personal Knowledge Regarding All Matters Noticed.

5A.12[2] PMK Need Not Be a Single Individual.

5A.12[3] Organization Must Provide Testimony As to All Information Reasonably Available to It on Noticed Topics.

5A.12[4] PMK Designee May Be Deposed Again As Natural Person.

5A.13 PMK Deposition Notice Must Be Drafted.

5A.13[1] Deposition Notice Must Be Written.

5A.13[2] Organization Must Be Identified As Deponent.

5A.13[3] Notice Must Specify a Place Authorized for Deposition of an Organization.

5A.13[4] Notice Must Specify Date and Time of Deposition.

5A.13[5] Notice Must Specify Scope of Deposition.

5A.13[5][a] Notice Must Describe Areas for Questioning With Reasonable Particularity.

5A.13[5][b] Deposition May Encompass Any Discoverable Subject.

5A.13[6] Notice May Require Production of Documents or Tangible Things.

5A.14 Deposition Notice Must Be Served.

5A.14[1] All Parties Must Be Served.

5A.14[2] Plaintiff May Serve Notice at Any Time After 20 Days After Service of Summons.

5A.14[3] Defendant May Serve Notice at Any Time.

5A.14[4] Service Must Be Made by Authorized Method.

5A.14[4][a] Methods for Service on Parties.

5A.14[4][b] Methods for Service on Non-Parties.

5A.15 Deposition Must End Before Discovery Cut-Off Date.

5A.16 CHECKLIST: Taking a Pre-Discovery ESI Systems PMK Deposition.

5A.17 Objective and Strategy.

5A.18 Counsel Should Seek Information to Assemble ESI Systems Menu.

5A.19 Counsel Should Seek ESI Menu Through Meet and Confer Process Before Issuing Pre-Discovery PMK Deposition Notice.

5A.20 PMK Deposition Is Usually Faster and Less Expensive Than Using Interrogatories.

5A.21 Drafting Pre-Discovery ESI Systems PMK Deposition Notice: Reasonable Particularity Requirement.

5A.22 Technical Assistance With Preparation and Deposition Is Essential.

5A.23 Preparing to Take a Pre-Discovery ESI Systems Deposition.

5A.23[1] Counsel Should Prepare a Deposition Outline.

5A.23[2] Counsel Should Prepare to Question PMK on Both Organization's ESI and Key Individuals' ESI.

5A.23[2][a] General Categories of ESI Important to Litigation.

5A.23[2][b] ESI Created and Maintained by "Key Players."

5A.23[2][c] ESI Maintained by the Organization.

5A.23[3] Counsel Should Inquire Regarding Document Retention Policies and Practices.

5A.23[4] Counsel Should Inquire Regarding Backup Tapes.

5A.24 Counsel Should Use Results of PMK Deposition to Draft ESI Discovery Demands.

5A.25 CHECKLIST: Taking a PMK Deposition During Discovery--Deposing PMK Regarding a Particular ESI System

5A.26 Objective and Strategy.

5A.27 Counsel Must Frame Specific Questions in Deposition Notice.

5A.27[1] Counsel Must Determine Goals of Deposition.

5A.27[2] Deposition Notice Must Be Drafted to Comply With Reasonable Particularity Requirement.

5A.28 Counsel Should Consider Including Document Request in Notice.

5A.29 Counsel May Take Deposition at Place Where System Can Be Demonstrated.

5A.30 Counsel May Take Experts to Deposition.

5A.31 Counsel Should Prepare Checklist for Taking Deposition.

5A.32 Counsel May Pursue Further Options With Respect to Unanswered Questions.

5A.33 CHECKLIST: Taking a Post-Discovery PMK Deposition--Deposing PMK Regarding ESI Discovery Responses; Positioning for Sanctions

5A.34 Objective and Strategy.

5A.35 Deposition Usually Is Contentious and Aggressive.

5A.36 Technical Assistance Throughout Entire Process Is Essential.

5A.37 Counsel Should Prepare Checklist for Taking Deposition.

5A.37[1] Counsel Should First Review Available Types of Sanctions.

5A.37[2] Counsel Should Review Statutory List of Acts Constituting Misuse of Discovery Process.

5A.37[3] Checklist Should Walk Deponent Through Prior Steps Taken in E-Discovery.

5A.38 CHECKLIST: Defending an ESI-Related PMK Deposition.

5A.39 Objective and Strategy.

5A.40 Calendar Response Period Immediately Upon Receipt of Deposition Notice.

5A.40[1] Written Objections to Deposition Notice Must Be Filed No Later Than Three Calendar Days Prior to Deposition.

5A.40[2] Time Extension Should Be Obtained Immediately if Necessary for Adequate Preparation.

5A.41 Attacking the PMK Notice.

5A.41[1] Counsel Should Examine and Resolve Any Problems With Deposition Notice.

5A.41[2] Deposition Notice May Not Identify a Natural Person.

5A.41[3] Deposition Notice Must Describe Scope of Examination With "Reasonable Particularity."

5A.41[4] Place of Deposition Must Be One Authorized by Statute.

5A.41[5] Counsel May Seek to Meet and Confer Regarding Notice Flaws.

5A.42 Counsel May File Motions to Stay, Quash, or for a Protective Order.

5A.42[1] Counsel May Seek These Remedies If Meet and Confer Is Unsuccessful.

5A.42[2] Motion to Stay and Quash a Deposition Notice Provides a Temporary Halt.

5A.42[3] Motion For a Protective Order Provides a Permanent Halt.

5A.43 Organization Has Duty to Conduct Reasonable Investigation.

5A.44 Organization Must Select Suitable PMK(s).

5A.44[1] Organization Designates Its Own PMK(s).

5A.44[2] PMK Need Not Have Pre-Existing Knowledge of Subject Matter.

5A.44[3] Designated PMK Should Be Good Spokesperson for Organization.

5A.45 Organization Must Educate PMK.

5A.45[1] PMK Is Required to Know All Information Reasonably Available to Organization.

5A.45[2] Checklist for Selecting and Educating PMK.

5A.45[3] Counsel Should Allow Sufficient Preparation Time.

5A.46 Deposition Procedure.

5A.46[1] Normal Deposition Procedures Apply.

5A.46[2] Counsel Should Object to Questions Beyond Scope of Deposition Notice.

5A.47 Deposition Notice for ESI Systems PMK Deposition.

5A.48 Letter From Deponent's Attorney Proposing Meet and Confer Process to Narrow Scope of PMK Deposition.

5A.49 Checklist for Taking Pre-Discovery IT Systems PMK Deposition.

5A.50 Checklist for Preparing PMK Deponent.

Diane E. Barry, Esq. n*

FOOTNOTES:

(n11)Footnote *. Diane E. Barry, Esq., is the Director of Discovery Strategy & Management at International Litigation Services, Inc. Diane's practice focuses on ESI discovery under state and federal rules of civil procedure, and complex litigation discovery planning and management. Diane assists clients in planning and preparing for ESI discovery conferences and court appearances, as well as preparation for specialized discovery such as IT custodian depositions, key player and IT interviews. In addition, Diane has significant expertise in utilizing technology to improve results in privilege and relevance review. Diane earned her A.B. degree from Vassar College and her J.D. degree, cum laude, from the Boston University School of Law. She holds a professional certification in data warehousing from U.C. Berkeley.

The author would like to acknowledge the assistance of Albert Barsocchini in the preparation of this chapter. Mr. Barsocchini, Assistant General Counsel and Senior Director at Guidance Software, is a recognized expert in electronic discovery and computer forensics. He served as Chairperson of the California State Bar's Law Practice Management & Technology Section in 2000. He is a founding member of the California State Bar Cyberspace Law Committee and currently serves as a special master for the State Bar of California in search and seizure of privileged and confidential matters. He received his J.D. from McGeorge School of Law, Sacramento, California.



2 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

I. STRATEGY

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.01

AUTHOR: Diane E. Barry, Esq.

5A.01 Scope.

This chapter covers three types of "person most knowledgeable" (PMK) depositions that are particular to e-discovery practice:

- The pre-discovery deposition of the PMK regarding a party's ESI systems.
- The deposition of a PMK regarding a specific complex system.
- The ESI discovery response PMK deposition, utilized to position a matter for significant discovery sanctions.

Core Statutes:

CCP §§ 2023.010, 2025.220, 2025.230, 2025.610; Evid Code § 771(a)



3 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

I. STRATEGY

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.02

AUTHOR: Diane E. Barry, Esq.

5A.02 Objective and Strategy.

This chapter discusses taking the deposition of the opponent's "person most knowledgeable" about the opponent's ESI systems. The phrase "person most knowledgeable" does not actually appear in the governing California statutes, but is in general use among practitioners. It describes the individual who is most qualified to testify on behalf of a deponent that is not a natural person regarding a particular matter [see CCP § 2025.230]; in the case of ESI, it is the person who is most qualified to testify regarding the existence and storage of ESI and the features of the company's data storage systems. This chapter provides tips and practice pointers regarding the strategic uses of such depositions, and how to take and prepare for them.

- The pre-discovery PMK deposition [see 5A.16 et seq.] is used to make up for a poor showing by the opposition at the early meeting of counsel mandated by Cal Rules Ct, Rule 3.274. One of the goals of the early meeting of counsel is to set out a menu of the available ESI, so that counsel can discuss which items are relevant and material, and pointed discovery can be drafted and issued [see discussion in Ch. 5, *Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference*, 5.14 et seq.]. *If opposing counsel is tardy in providing such a menu, counsel should not wait.* Counsel should proceed to obtain the information necessary to create the menu by taking a pre-discovery deposition of the PMK regarding the opposition's computer systems. Waiting creates additional discovery problems. For example, the desired data can be gone; the opposition may collect and process it in ways that will impose additional costs on the other participants. Most importantly, judicial precedent shows that ESI discovery requests that demand specific data items are most likely to be enforced.

- It may be necessary to depose a PMK during discovery to obtain more information about a specific system [see 5A.25 et seq.]. As e-discovery progresses, it can become apparent that additional information may be required in order to make good use of ESI available from a particular system. The system may be complex, and/or the organization has customized it to the point where it no longer functions like its off-the-shelf brethren, or other issues may require clarification. If more information is required as to a particular system either to find out whether the system should be discoverable, or to make efficient use of the information, this deposition is essentially a training session with someone who knows the system well.

■ The post-discovery PMK deposition [see 5A.33 et seq.] is a strategic part of positioning a matter for significant discovery sanctions. The goal of the post-discovery PMK deposition is to attack inadequate e-discovery responses and obtain improved responses, or sanctions for discovery abuse, or both. This deposition can be taken at almost any point after formal discovery responses have commenced, when an inadequate response has been delivered, discovery deadlines are being missed, or the other side is delaying the discovery in a significant way. Sanctions can consist of monetary sanctions, orders to produce, evidentiary advantages, and (in extreme cases) dismissal of the action or striking of claims and defenses.

This chapter is intended to assist counsel in deciding whether or not to take PMK depositions, to prepare for or defend such a deposition, and to make use of the fruits of the deposition once taken.



Strategic Point--Get Technical Assistance Early.

All of the PMK depositions outlined in this chapter are technical in nature. The deponent will be talking about information technology architecture, software, storage decisions, and other technical matters. It is *strongly* recommended that counsel involved with this kind of deposition--either taking or defending--obtain technical support as early in the process as possible. Counsel will need a technical consultant to help in drafting the notice, which outlines the areas for questioning, as well as in drafting a deposition outline. Counsel should also plan to take a technical consultant to the deposition. Even if good preparation has enabled counsel to understand the questions being asked, counsel will need to understand the answers a technical deponent gives at the deposition. It can also cut back on an embittered deponent's occasional temptation to talk in technical circles around a non-technical person.



Cross References:

Sanctions in e-discovery, see Ch. 13, Seeking or Opposing Sanctions for Noncompliance.

Discovery sanctions generally, see Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 3, Sanctions.

Deposition practice and procedure generally, see Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 6, Oral Depositions in California; Ch. 7, Oral Depositions Outside California.



4 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

II. COMPLYING WITH LEGAL REQUIREMENTS FOR TAKING A "PERSON MOST KNOWLEDGEABLE" DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.03

AUTHOR: Diane E. Barry, Esq.

5A.03 CHECKLIST: Complying With Legal Requirements for Taking a "Person Most Knowledgeable" Deposition

- ☐ Obtain technical expert or other consultant to assist in strategy and preparation of PMK notice and deposition outline.

Discussion:

See 5A.02, 5A.22, 5A.36

- ☐ Is opponent a corporation or other legally recognized artificial person?

Authority:

CCP § 2025.230

Discussion:

See 5A.05, 5A.06

- ☐ Make sure that timing is correct for issuance of deposition notice.
- ☐ Defendants may serve notice of deposition at any time after earlier of having been served or having appeared in the action.
- ☐ Generally, plaintiffs may serve deposition notices on any date 20 days after either:
- ☐ Service of summons on any defendant; or

☐ Appearance by any defendant.

Authority:

CCP § 2025.210

Discussion:

See 5A.14[2], [3]

☐ Consider meeting and conferring with opposing counsel to obtain desired ESI discovery information through other means, within an acceptably short time period.

Authority:

CCP §§ 2023.010(c), 2023.020; Parker v. Wolters Kluwer United States, Inc. (2007) 149 CA4th 285, 294, 57 CR3d 18 (failure to meet and confer, even without any other discovery abuses, is a sufficient basis for imposition of monetary sanction)

Discussion:

See 5A.19

☐ If opposing counsel refuses to meet and confer regarding provision of ESI discovery information without resort to deposition, consider bringing motion for sanctions for discovery abuse.

Authority:

CCP §§ 2023.010, 2023.020; Parker v. Wolters Kluwer United States, Inc. (2007) 149 CA4th 285, 294, 57 CR3d 18 (failure to meet and confer, even without any other discovery abuses, is a sufficient basis for imposition of monetary sanction)

Discussion:

See Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferring, and Case Management (duty to meet and confer), Ch. 13, Seeking or Opposing Sanctions for Noncompliance

☐ If opposing counsel is willing, consider holding informal conference with opposing counsel and opponent's IT personnel (no court reporter) to obtain the necessary information.

Authority:

CCP §§ 2023.010(c), 2023.020; Parker v. Wolters Kluwer United States, Inc. (2007) 149 CA4th 285, 57 CR3d 18 (failure to meet and confer, even without any other discovery abuses, is a sufficient basis for imposition of monetary sanction)

Discussion:

See 5A.19

☐ Decide whether to depose a particular person or position holder, or to have the corporate opponent select and educate an agent who can answer questions.

Authority:

CCP § 2025.230, Maldonado v. Superior Court (2002) 94 CA4th 1390, 1395-1397, 115 CR2d 137

(discussing corporate litigant's duties in selecting and educating a PMK for deposition)

Discussion:

See 5A.05, 5A.06

- ☐ Consider requesting production of documents at deposition--including access to known target ESI systems.

Authority:

CCP § 2025.230

Discussion:

See 5A.08

Form:

See 5A.47, Deposition Notice for ESI Systems PMK Deposition.

- ☐ Draft PMK deposition notice, including time and location, specific description of areas for questioning, and description of any documents that should be made available at deposition.

Authority:

CCP § 2025.230

Discussion:

See 5A.10, 5A.11, 5A.13

Form:

See 5A.47, Deposition Notice for ESI Systems PMK Deposition.

- ☐ Do not attempt to specify a particular person to attend on behalf of organization.

Authority:

CCP § 2025.230

Discussion:

See 5A.06, 5A.13[2]

- ☐ Serve deposition notice on every party to the action, in accordance with time requirements applicable to that party.

Authority:

CCP §§ 1013, 2015A.050, 2020.220, 2025.210, 2025.240; see CCP § 2025.610

Discussion:

See 5A.13

- ☐ Complete deposition on or before 30th day prior to trial.

Authority:

CCP § 2024.020(a)

Discussion:
See 5A.15



5 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

II. COMPLYING WITH LEGAL REQUIREMENTS FOR TAKING A "PERSON MOST KNOWLEDGEABLE"
DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.04

AUTHOR: Diane E. Barry, Esq.

5A.04 Objective and Strategy.

All PMK depositions have certain common features and are subject to common statutory requirements. Counsel, whether seeking to take or defending a PMK deposition, must be aware of these features and requirements regardless of the content, timing, or tactical goals of the particular deposition. The goal of this part is to acquaint counsel with the basic features of PMK depositions, as authorized by *CCP* § 2025.230.



6 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

II. COMPLYING WITH LEGAL REQUIREMENTS FOR TAKING A "PERSON MOST KNOWLEDGEABLE" DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.05

AUTHOR: Diane E. Barry, Esq.

5A.05 CCP § 2025.230 Authorizes Taking Deposition of Organization Rather Than a Specific Natural Person.

CCP § 2025.230 authorizes taking the deposition of a corporation (or other entity) rather than of a natural person. This section is useful when the identity of the person or persons at the organization in possession of the desired information is unknown or in question. The corporate party is obligated to conduct a reasonable investigation, and to produce a person or persons who can testify on behalf of the organization on the subjects described in the deposition notice.

Consider:

Prior to *CCP § 2025.230*, it was necessary for the noticing party either to guess who might possess the knowledge desired, or to take multiple depositions of corporate employees, asking each if they had any knowledge of the subject. The problems with this practice are clear: The guesses were often wrong, and taking that many depositions clearly wasted both time and resources. The multiple employee approach also led to finger pointing--"you should have asked this question of that other deponent." *CCP § 2025.230* increases discovery efficiency by placing the onus on the corporate party to identify and produce someone who can provide the desired testimony [*CCP § 2025.230*; *Maldonado v. Superior Court* (2002) 94 CA4th 1390, 1395, 115 CR2d 137 ("[t]he purpose of this provision is to eliminate the problem of trying to find out who in the corporate hierarchy has the information the examiner is seeking.")].

Form:

See 5A.47, Deposition Notice for ESI Systems PMK Deposition.



7 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

II. COMPLYING WITH LEGAL REQUIREMENTS FOR TAKING A "PERSON MOST KNOWLEDGEABLE" DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.06

AUTHOR: Diane E. Barry, Esq.

5A.06 PMK Deposition Notice Cannot Specify Deposition of a Particular Person.

CCP § 2025.230 authorizes the recipient organization to specify those of "its officers, directors, managing agents, employees, or agents" who are "most qualified" to testify on its behalf regarding the listed areas of inquiry. *The organization selects the deposition designee, not the noticing party.* This means that the party issuing the notice cannot object to the designee unless and until the designee proves unable to respond to the noticed areas of inquiry.



Strategic Point

If the issuing party believes that someone else is better situated to respond to the questions, or believes that someone else has discoverable knowledge, the remedy is to notice an ordinary deposition of that person, rather than noticing a corporate PMK deposition [*CCP §§ 2025.220, 2025.230*].



8 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

II. COMPLYING WITH LEGAL REQUIREMENTS FOR TAKING A "PERSON MOST KNOWLEDGEABLE"
DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.07

AUTHOR: Diane E. Barry, Esq.

5A.07 PMK Deposition Notice Must Specify Deposition Topics With "Reasonable Particularity."

The PMK deposition notice must provide a "general description sufficient to identify the person or particular class to which the person belongs" and "describe with reasonable particularity the matters on which examination is requested" [CCP §§ 2025.220, 2025.230].

Form:

See 5A.47, Deposition Notice for ESI Systems PMK Deposition.



9 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

II. COMPLYING WITH LEGAL REQUIREMENTS FOR TAKING A "PERSON MOST KNOWLEDGEABLE"
DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.08

AUTHOR: Diane E. Barry, Esq.

5A.08 PMK Deposition Notice Can Request Production of Documents at Deposition.

Because the notice is directed to the organization, the designee must produce the documents reasonably available to the organization. The designee must search its own files, and either the PMK or the organization must make inquiries of other persons to obtain all described documents reasonably available to the organization [*CCP* §§ 2025.220(4), 2025.230; *Doppes v. Bentley Motors, Inc.* (2009) 174 CA4th 967, 973-974, 94 CR3d 802 (court granted motion to compel continued deposition and production of documents after PMK attended deposition without bringing documents specified in deposition notice)].



10 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

II. COMPLYING WITH LEGAL REQUIREMENTS FOR TAKING A "PERSON MOST KNOWLEDGEABLE"
DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.09

AUTHOR: Diane E. Barry, Esq.

5A.09 PMK Deposition Notice Must Specify If Testimony Will Be Recorded and If Recording May Be Used at Trial.

As with ordinary depositions, if the testimony is to be video or audio recorded, and if the noticing party wishes to reserve the right to use those recordings at trial, the notice must so specify [CCP § 2025.220].

Form:

See 5A.47, Deposition Notice for ESI Systems PMK Deposition.



11 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

II. COMPLYING WITH LEGAL REQUIREMENTS FOR TAKING A "PERSON MOST KNOWLEDGEABLE"
DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.10

AUTHOR: Diane E. Barry, Esq.

5A.10 No Specified Limits on Number of Topics That Can Be Noticed.

CCP § 2025.230 does not specify a limit on the number of topics that can be noticed in a PMK deposition. Neither does it require that the topics noticed be related in any way other than the general discovery requirement that the topics be reasonably calculated to lead to discovery of relevant information [*see CCP § 2017.010*].

However, the court is required to limit discovery if it determines that the burden, expense, or intrusiveness of that discovery clearly outweighs the likelihood that the information sought will lead to the discovery of admissible evidence. A truly lengthy topics list is likely to lead to a successful motion for a protective order [*CCP §§ 2017.020* (motions for protective order--limiting scope of discovery), 2025.420 (motion for a protective order--depositions), 2025.230].



Cross References:

Seeking protective order in e-discovery, see Ch. 11, Seeking or Opposing Protective Order.

General scope of discovery, see Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 2, Scope of Discovery.



12 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

II. COMPLYING WITH LEGAL REQUIREMENTS FOR TAKING A "PERSON MOST KNOWLEDGEABLE" DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.11

AUTHOR: Diane E. Barry, Esq.

5A.11 Place for Taking PMK Deposition.

5A.11[1] Place When Deponent Is a Party. If the target organization is a party to the action, the PMK deposition can be noticed for either of the following places, at the option of the noticing party [CCP § 2025.250(b)]:

- Within 75 miles of the organization's principal executive or business office in California; or
- Within the county where the action is pending and within 150 miles of that office.

Form:

See 5A.47, Deposition Notice for ESI Systems PMK Deposition.

5A.11[2] Place When Deponent Is Not a Party. If the organization is not a party, the deposition must be noticed for a place within 75 miles of the organization's principal executive or business office in California, if there is one. The organization can always consent to a more distant place [CCP § 2025.250(c)].

If the organization has not designated such an office in California, the noticing party may designate a place either in the county where the action is pending, or within 75 miles of *any* executive or business office of the organization in California [CCP § 2025.250(d)].

Form:

See 5A.47, Deposition Notice for ESI Systems PMK Deposition.



13 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

II. COMPLYING WITH LEGAL REQUIREMENTS FOR TAKING A "PERSON MOST KNOWLEDGEABLE" DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.12

AUTHOR: Diane E. Barry, Esq.

5A.12 Organization Must Identify, Educate, and Produce Person(s) "Most Qualified" to Testify As to All Reasonably Available Corporate Knowledge on Identified Subjects.

5A.12[1] PMKs Need Not Have Actual Personal Knowledge Regarding All Matters Noticed. *CCP § 2025.230* authorizes the organization to designate those of "its officers, directors, managing agents, employees, or agents" who are "most qualified" to testify on its behalf regarding the listed areas of inquiry. The designee must be able to testify "to the extent of any information known or reasonably available to the deponent." The deponent is the organization.

The practice in California usually has been for the organization to find a person or persons with at least some personal knowledge, and to offer one or more of them as PMK designee(s). However, California courts have explicitly held that the organization may not provide only the personal knowledge of PMK designees [*Maldonado v. Superior Court* (2002) 94 CA4th 1390, 1395-1397, 115 CR2d 137 (discussing corporate litigant's duties in selecting and educating a PMK for deposition)]. If there is corporate information beyond the personal knowledge of the designee(s), the organization is required to educate the selected PMK(s) as to additional information reasonably available to the organization, so that all information reasonably available to the organization is provided through the PMK(s).

Consider:

Despite the common practice of providing a designee with at least some personal knowledge, the specific language of *CCP § 2025.230* does not require that the corporate PMK designee have any pre-existing personal knowledge of the subject matter of the deposition. *CCP § 2025.230* requires only that the organization designate the officers, directors, managing agents, employees, or agents most qualified to testify for the organization. Under this rubric, the organization may choose an unknowledgeable "agent" who can then be thoroughly educated and designated to testify on the organization's behalf [*CCP § 2025.230*; *FRCP 30(b)(6)*; see *Maldonado v. Superior Court* (2002) 94 CA4th 1390, 1395-1397, 115 CR2d 137 (discussing corporate litigant's duties in selecting and educating a PMK for deposition)].

Strategic Point--Deponent:



CCP § 2025.230 authorizes the organization or other entity to choose its own spokesperson. In most other situations, an organization has no choice as to who testifies, inasmuch as a natural person must have personal experience of a subject in order to present valid testimony. *CCP § 2025.230* requires no such personal experience. *CCP § 2025.230* specifically authorizes the organization to educate one or more designees and provide them to testify. Thus, the deponent's counsel should consider the following questions:

- Who would the organization *like* to put on the stand?
- Who would make a good witness?

This is an excellent opportunity for counsel and client to consider carefully and choose strategically who can best present the organization's information regarding the noticed topics.

Cross References:

Selecting suitable PMKs, see 5A.44.

Selecting multiple PMKs, see 5A.12[2].

Educating PMKs, see 5A.45.

Checklist for qualifications of PMKs, see 5A.50.

5A.12[2] PMK Need Not Be a Single Individual. *CCP § 2025.230* specifically authorizes the organization to designate multiple persons to testify regarding noticed topics. This is often the best choice when, for example, the deposition notice asks about corporate practices across a time period. Different persons often will have personal knowledge of part of the time period, but not all. The organization can choose either to produce all of the knowledgeable persons, or educate someone as to the joint knowledge they all hold [*CCP § 2025.230*; *Maldonado v. Superior Court* (2002) 94 CA4th 1390, 1395-1397, 115 CR2d 137 (discussing corporate litigant's duties in selecting and educating a PMK for deposition)].



Strategic Point--Consider Joint Deposition:

It can be costly to produce multiple persons to testify on a topic, as each can require a separate deposition. It also creates the problem of finger pointing (for example, today's deponent says that yesterday's deponent is actually the one who knows about that topic). A joint deposition may be considered as a creative solution. Opposing counsel sometimes will agree to permit a joint deposition of all PMKs on a particular topic. When this is done, all of the PMKs typically are present and placed under oath, sitting together on one side of the table with opposing counsel. If one of the deponents wished to respond, he or she raises a hand, and the deponent's counsel calls upon them, in turn if more than one indicates they have knowledge about the question. If no one knows the answer, there is a clean record as to that fact, instead of trying to show that five different deponents at separate depositions each were unable answer the question or couldn't answer it completely. Conversely, counsel may wish for separate records and the expense may not be an issue. This is a strategic and budgetary option that should be considered by counsel.

5A.12[3] Organization Must Provide Testimony As to All Information Reasonably Available to It on Noticed Topics. Even if the organization identifies and produces deponent(s) with actual knowledge on the topics, its obligation

is not necessarily fully satisfied. The organization must provide a deponent or deponents who can respond, either singly or as a group, with *all* knowledge on the subjects that is reasonably available to the organization. In other words, the organization must examine its information sources and educate its designee(s) if more information is available in addition to their personal knowledge. The organization must examine its records, speak to employees and former employees, and gather its "knowledge" on the topics in the deposition notice. All such information should be made available to the opposition through the testimony of the PMK designee(s). If the designee(s) cannot testify as to all of this information from their natural recollection, at least one designee must be educated as to such materials, so that their testimony can fully present the information available to the organization [*CCP § 2025.230*; *Maldonado v. Superior Court (2002) 94 CA4th 1390, 1395-1397, 115 CR2d 137* (discussing corporate litigant's duties in selecting and educating a PMK for deposition)].

Example--Duty to Educate PMK Designee.

The plaintiff noticed PMK depositions regarding three topics having to do with termination of petitioners employment. The defendant organization was in bankruptcy, and no current employees had good knowledge of the documents and events described. The organization provided deponents from the human relations department and other corporate officers who among them still could not answer the bulk of plaintiff's questions. Neither the organization nor the deponents conducted a thorough investigation to locate persons who could speak to the events described in the notice, or even to locate all documents reasonably available on the topics. The court held that the defendant had not properly responded to the PMK deposition notice. It held that *CCP § 2025.230* did not permit the organization to rely upon the recollection of the individuals. The organization was required to conduct an investigation to gather the information reasonably available to the organization, so that the deponents could be educated on those points, and could offer the plaintiff PMK testimony that would present all information reasonably available to the organization [*Maldonado v. Superior Court (2002) 94 CA4th 1390, 115 CR2d 137*] .

5A.12[4] PMK Designee May Be Deposed Again As Natural Person. The fact that a person was provided as the PMK designee does not bar taking that person's deposition again, in the person's own name, as the deposition of a natural person, at a later date [*CCP § 2025.610(c)(1)*].

Example--Re-deposing the PMK Designee As a Natural Person:

Mr. Jones is the current Accounting Manager of a corporate defendant. Plaintiff sent the defendant organization a deposition notice under *CCP § 2025.230* requesting the deposition of a PMK regarding the organization's practices as to booking sales revenue in the year 2007. The organization provided Mr. Jones as the PMK designee for this topic. In addition, Mr. Jones is a percipient witness of facts and events relevant to the litigation matter. Under *CCP § 2025.610(c)(1)*, plaintiff may take Mr. Jones' deposition again later in the action by issuing an ordinary deposition notice, naming him specifically as the deponent.



14 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

II. COMPLYING WITH LEGAL REQUIREMENTS FOR TAKING A "PERSON MOST KNOWLEDGEABLE" DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.13

AUTHOR: Diane E. Barry, Esq.

5A.13 PMK Deposition Notice Must Be Drafted.

5A.13[1] Deposition Notice Must Be Written. A party desiring to take the oral deposition of any person must give notice in writing of the taking of the deposition [CCP § 2025.220(a)].

Cross Reference:

General requirements for deposition notices, see *Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 6, Oral Depositions in California, 6.03 et seq.*

Form:

See 5A.47, Deposition Notice for ESI Systems PMK Deposition.

5A.13[2] Organization Must Be Identified As Deponent. The notice must include the name of each deponent, and the address, if known, of any deponent who is not a party to the action [CCP § 2025.220(a)(3)]. CCP § 2025.230 authorizes the deposition of an organization, and not of a natural person. Therefore, the deposition notice must specify the deposition of the organization. It may not attempt to require that the organization produce a particular person to answer PMK type questions [CCP § 2025.230].

Cross Reference:

General requirements for deposition notices, see *Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 6, Oral Depositions in California, 6.03 et seq.*

Form:

See 5A.47, Deposition Notice for ESI Systems PMK Deposition.

5A.13[3] Notice Must Specify a Place Authorized for Deposition of an Organization. The notice must specify an address where the deposition will be taken [CCP § 2025.220(a)(1)]. The places authorized for the deposition of an organization are different from those of a natural person [see discussion in 5A.11]. Generally, if the deponent organization is a party, the place specified in the notice must be within 75 miles of the organization's principal executive

or business office in California, or within the county where the action is pending and within 150 miles of that office [CCP § 2025.250].

Form:

See 5A.47, Deposition Notice for ESI Systems PMK Deposition.

5A.13[4] Notice Must Specify Date and Time of Deposition. The deposition notice must specify the date of the deposition and the time it will commence [CCP § 2025.220(a)(2)].



Timing--At Least 10 Days After Service of Notice.

An oral deposition must be scheduled for a date at least 10 days after service of the deposition notice [CCP § 2025.270].

5A.13[5] Notice Must Specify Scope of Deposition.

5A.13[5][a] Notice Must Describe Areas for Questioning With Reasonable Particularity. A PMK deposition notice must describe with "reasonable particularity the matters on which examination is requested" [CCP § 2025.230]. In the case of an ESI related deposition, counsel should specify the systems that are of interest, what it is about the systems that are of interest, and the time frame of interest. This kind of drafting should be done with the active assistance of a technical expert who can assist counsel in specifying what information is needed to move the case forward, and how to describe it with particularity [CCP §§ 2017.010, 2025.010].

5A.13[5][b] Deposition May Encompass Any Discoverable Subject. A noticing party is permitted request deposition testimony from an organization on any subject that is relevant and not privileged [CCP §§ 2017.010, 2025.010].



Strategic Point--Designating Area for Questioning:

Counsel does not need to know how a particular question can be answered in order to designate it as an area for questioning. It is up to the other side to figure out how something happened, or what was done, or to admit that they don't know. If the other side admits that they don't know how something happened, it is prudent for counsel to get it in writing.

Examples:

- The author once specified, as an area for questioning, how a particular computer came to be "unavailable" for discovery, as stated in the other side's discovery response. (It turned out to be at the bottom of a lake.)
- Likewise the author has asked for a PMK who could show how particular accounting numbers were created using the organization's accounting system, as claimed by the opponent, and for a demonstration of the wiping technique the organization claimed to use for recycling executive computers.

5A.13[6] Notice May Require Production of Documents or Tangible Things. The notice must specify with reasonable particularity any materials or category of materials to be produced by the deponent [CCP § 2025.220(a)(4)].

The noticing party can require that the deponent produce any document or tangible thing for inspection and copying at the deposition [CCP § 2025.280]. If the documents to be produced are consumer or employee records, the noticing party may need to give additional notice to the consumer or employee who is the subject of the records [see CCP §§

1985.3, 1985.6, 2020.410(d)].



Strategic Point--Request Documents Used by Opponent in Deposition Preparation:

Counsel should include in the deposition notice a request for all documents reviewed in preparation for the deposition. Those documents are subject to discovery, especially if they refreshed the recollection of the deponent [see *Evid Code* § 771 and discussion in 5A.08]. For PMKs, the organization is required to conduct a reasonable investigation and educate its PMK on all corporate knowledge on the noticed topics [CCP § 2025.230]. The organization often conveys such information to its PMK through documents--documents that created or "refreshed" the corporate recollection. Counsel should ask for them in the deposition notice.



15 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

II. COMPLYING WITH LEGAL REQUIREMENTS FOR TAKING A "PERSON MOST KNOWLEDGEABLE" DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.14

AUTHOR: Diane E. Barry, Esq.

5A.14 Deposition Notice Must Be Served.

5A.14[1] All Parties Must Be Served. The CCP requires only that a deposition notice be served on every party who has *appeared* in the action [CCP § 2025.240(a)]. As a practical matter, however, the notice should be served on *any* other party who has been served with summons, to avoid having a later-appearing party assert that he or she is entitled to take a subsequent deposition of the same deponent because of a lack of notice of the original deposition [see CCP § 2025.610].

5A.14[2] Plaintiff May Serve Notice at Any Time After 20 Days After Service of Summons. A plaintiff may serve a deposition notice without leave of court on any date that is 20 days after the service of the summons on, or appearance by, any defendant [CCP § 2025.210(b)]. A plaintiff may move, with or without notice, for leave of court to serve a deposition notice at an earlier date [CCP § 2025.210(b)]. The plaintiff must demonstrate good cause [CCP § 2025.210(b)].

5A.14[3] Defendant May Serve Notice at Any Time. A defendant may serve a deposition notice without leave of court at any time after that defendant has been served or has appeared in the action, whichever occurs first [CCP § 2025.210(a)].

5A.14[4] Service Must Be Made by Authorized Method.

5A.14[4][a] Methods for Service on Parties. A deposition notice may be served by mail, express mail, or another method of overnight delivery. If the parties agree in writing, service also may be made by facsimile transmission [CCP §§ 1013, 2015A.050]. If served by mail, the deposition notice may be served by an attorney, but may not be served by a party to the action [CCP § 1013a].

Cross Reference:

Service of deposition notice, see *Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 6, Oral Depositions in California*, 6.11.

5A.14[4][b] Methods for Service on Non-Parties. A deposition subpoena compelling attendance of a nonparty deponent at a deposition must be personally served, but it may be served by any person, including a party [*CCP* § 2020.220(b)].



16 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

II. COMPLYING WITH LEGAL REQUIREMENTS FOR TAKING A "PERSON MOST KNOWLEDGEABLE"
DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.15

AUTHOR: Diane E. Barry, Esq.

5A.15 Deposition Must End Before Discovery Cut-Off Date.

Discovery must be completed on or before the 30th day prior to the date initially set for trial. All motions regarding discovery must be heard on or before the 15th day prior to the date initially set for trial [*CCP* § 2024.020(a)].

Discovery is "complete" on the day a response is due or on the day a deposition begins [*CCP* § 2024.010].



17 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

III. TAKING A PRE-DISCOVERY ESI SYSTEMS PMK DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.16

AUTHOR: Diane E. Barry, Esq.

5A.16 CHECKLIST: Taking a Pre-Discovery ESI Systems PMK Deposition.

- ☐ Obtain technical expert or other technical consultant to assist in:
- ☐ Assessing adequacy of any proffered ESI systems information.
 - ☐ Assessing completeness of ESI productions.
 - ☐ Assist with ESI System PMK deposition notice (preparing or attacking).
 - ☐ Assist with ESI System PMK deposition preparation (taking or defending).

Discussion:

See 5A.18, 5A.22

Form:

See 5A.49

- ☐ Evaluate whether opposing parties produced sufficient information at early meeting of counsel to permit drafting of specific discovery requests.

Authority:

CCP §§ 2023.010(c), 2023.020; *Cal Rules Ct, Rule 3.724*; *Zubulake v. UBS Warburg (2003) 217 FRD 309, 322* (first of seven criteria for judicial enforcement of document demands is specificity of the demand).

Discussion:

See 5A.17-5A.19

Form:

5A.49 (PMK deposition checklist); see also 5.30 (meet and confer checklist)

- ☐ If opposing counsel did not provide sufficient description of all available ESI at early meeting of counsel, attempt to meet and confer with opposing counsel to obtain necessary information within an acceptable time period.

Authority:

CCP §§ 2023.010(c), 2023.020; *Parker v. Wolters Kluwer United States, Inc.* (2007) 149 CA4th 285, 57 CR3d 18

Discussion:

See 5A.19

Form:

See 5A.48

☐ Time period for attempting to obtain information by informal resolution before resorting to PMK deposition usually should be no more than one month.

☐ All informal efforts should be fully documented.

- ☐ If desired description of available ESI cannot be obtained through early meeting of counsel or through meet and confer efforts, evaluate strategic necessity and/or desirability of taking ESI systems PMK deposition.

Authority:

CCP §§ 2025.220, 2025.230, 2025.240

Discussion:

See 5A.16, 5A.19, 5A.20

☐ Include assessment of monetary costs of PMK deposition to client.

- ☐ If information is necessary and worth the cost, prepare and serve ESI systems PMK deposition notice.

Authority:

CCP §§ 2025.220, 2025.230, 2025.240

Discussion:

See 5A.23

Form:

See 5A.47

- ☐ Calendar time to prepare deposition notice with assistance from technical consultant.

Authority:

CCP §§ 2025.220, 2025.230, 2025.240

Discussion:

See 5A.22, 5A.23[2]

- ☐ Calendar time to prepare for deposition with assistance from technical consultant.

Authority:

CCP §§ 2025.220, 2025.230, 2025.240

Discussion:

See 5A.14, 5A.22, 5A.23

Form:

See 5A.49



18 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

III. TAKING A PRE-DISCOVERY ESI SYSTEMS PMK DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.17

AUTHOR: Diane E. Barry, Esq.

5A.17 Objective and Strategy.

A pre-discovery ESI PMK deposition should be designed to make up for a poor early meeting of counsel. *Cal Rules Ct, Rule 3.724(8)* lists ESI-related topics that counsel are supposed to address at the early meet and confer meeting of counsel prior to the case management conference. Reduced to its essentials, counsel is required to provide information regarding all ESI available for discovery and to discuss any issues that might affect ESI production. The result should be that counsel walk away from this early meeting of counsel with an "ESI menu"--that is, a listing of all available ESI and an understanding of the issues regarding the production of any particular items. This ESI menu is intended to assist counsel in making informed agreements regarding discovery scope, deadlines, and related issues. It also is extremely helpful to counsel who wish to draft specific and enforceable inspection demands.

If the early meeting of counsel did not provide the information required, the most appropriate and efficient remedy is to notice and take the deposition of the other side's person most knowledgeable regarding their ESI systems [*CCP* §§ 2023.010, 2023.020, 2025.230, CRC 3.274, Form 5.30].



Strategic Point--Move Quickly:

If opposing counsel comes to the meet and confer unprepared, and/or does not provide enough information to prepare an ESI menu, counsel should not wait. Counsel must move swiftly to acquire the information needed to assemble such a menu, so that discovery can progress. Data problems, if there are any, will not improve with elapsing time. If the other side came unprepared, they may not be preserving all relevant ESI, or may not be putting it into a speedy production mode.



Warning:

Broad ESI requests are an open invitation to opposing counsel to produce everything asked for and thereby bury the requesting counsel in an ocean of minimally relevant data. In addition, an ESI request that demands "all ESI relevant to the subject matter of the complaint" stands little chance of receiving either good judicial enforcement or a tidy response. Contrast this with a request that demands "all e-mails to and from named natural persons, from both the corporate Microsoft Exchange Server, and the individual's laptops, and the corporate Blackberry server; which were sent or received during a specified

time frame," perhaps with listed terms appearing in the e-mail body or subject line, and adding, "Please provide similar e-mails from the organization's backup tapes for the following listed former employees."

Without the ESI menu of the kind that is supposed to change hands at the early meeting of counsel, this kind of specific demand is almost impossible to draft. The ESI menu is most useful when obtained *before* attempting to draft ESI inspection requests [see *Zubulake v. UBS Warburg (SDNY 2003) 217 FRD 309, 322-323* (specificity is first and most important of seven listed criteria guiding judicial enforcement of ESI requests)].

**Cross References:**

Detailed discussion of meet and confer process, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference, 5.14et seq., 5.30* (checklist).

Drafting demand for production of ESI, see *Ch. 6, Demanding Production of Electronically Stored Information in California Court*.



19 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

III. TAKING A PRE-DISCOVERY ESI SYSTEMS PMK DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.18

AUTHOR: Diane E. Barry, Esq.

5A.18 Counsel Should Seek Information to Assemble ESI Systems Menu.

The information necessary to assemble an ESI systems menu is the same kind of information that *Cal Rules Ct, Rule 3.724(8)* requires counsel to discuss in the meet and confer process. In particular, counsel are required to discuss, and report to the court on, "any other issues relating to the discovery of electronically stored information, including developing a proposed plan relating to the discovery of the information."

The kind of information needed to assemble the ESI systems menu is the same kind of information obtained from counsel's own client during the initial ESI systems interview(s), which ought to have occurred at the commencement of the engagement. The menu should address at least two kinds of ESI:

- The ESI kept by each of the natural person "key players" involved in the subject matter of the litigation; and
- The ESI kept by the organization.

From this "menu," which ought to detail all of the relevant ESI available, counsel can issue specific ESI requests, demanding only the ESI that will actually be of use to the client's case.



Cross References:

Client interviews to determine what ESI exists, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference*, 5.03 et seq.

Matters required to be discussed at early meet and confer meeting of counsel, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference*, 5.19, 5.30 (checklist).



20 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

III. TAKING A PRE-DISCOVERY ESI SYSTEMS PMK DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.19

AUTHOR: Diane E. Barry, Esq.

5A.19 Counsel Should Seek ESI Menu Through Meet and Confer Process Before Issuing Pre-Discovery PMK Deposition Notice.

If the early meeting of counsel fails to produce the desired ESI menu, counsel should immediately begin a meet and confer effort to obtain the information within a reasonable amount of time after the early meeting. Counsel always has a duty to meet and confer in good faith regarding discovery disputes. Thus, counsel should initiate such an effort before taking a PMK deposition.

Strategic Points:



- An ESI systems PMK deposition notice often results in a motion for a protective order. Counsel defending the PMK notice need to show that reasonable attempts were made to obtain the information as part of the meet and confer process, and that those reasonable attempts failed. Documented informal attempts to obtain the necessary information will help in making the necessary showing.
- If the sides are not already impossibly aggressive and entrenched, consider receiving the information informally, at a conference at opposing counsel's offices with the IT custodian(s) present to answer questions. If counsel have a good working relationship, and/or if costs are an issue, this approach can work well. The noticing counsel can bring an IT expert to assist them in asking questions. Sometimes, these conferences become a speedy conversation among the technical persons, with counsel taking notes. The advantage of this approach is speed and lowered costs. Since it is informal, opposing counsel often will allow the meeting sooner than a formal deposition. It also avoids the costs of a court reporter, formal deposition preparation, and related costs. The disadvantage is that there will be no formal record of questions that can be attached to a motion to compel if questions remain unanswered or if the process breaks down.



Warning:

Don't let it drag on. If counsel is unable to obtain a good menu, or at least a good start on a good ESI

menu, within a few weeks after the early meeting of counsel, counsel should issue an ESI systems PMK deposition notice [CCP §§ 2025.230, Cal Rules Ct, Rule 3.274; see CCP §§ 2023.010(c), 2023.020; *Nicholas v. Wyndham Int'l, Inc.*, (4th Cir 2004) 373 F3d 537 (third-party ESI custodian deposition quashed as plaintiffs were apparently complying with their discovery obligations and deposition seemed cumulative and burdensome under the circumstances); but see *Nat'l Life. Ins. Co. v. Hartford Accident & Indem. Co.* (3d Cir. 1980) 615 F2d 595, 600 ("[t]here are strong reasons why a party strategically selects to proceed by oral deposition rather than alternate means, including the spontaneity of witness responses"); *Zamora v. D'Arrigo Brother Co.*, (ND CA) 2006 US Dist. LEXIS 83106 ("[n]o rule requires plaintiffs to pursue every possible alternative before noticing a 30(b)(6) deposition")].



21 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

III. TAKING A PRE-DISCOVERY ESI SYSTEMS PMK DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.20

AUTHOR: Diane E. Barry, Esq.

5A.20 PMK Deposition Is Usually Faster and Less Expensive Than Using Interrogatories.

If the ESI menu is not forthcoming during the early meeting of counsel, or fairly immediately thereafter, the PMK deposition is the next best available discovery vehicle for obtaining it. Interrogatories can take months of meeting and conferring and complaining to the discovery referee or the court and motions to compel, etc., in order to obtain any kind of response. Moreover, even after months of law and motion practice, counsel can still be left without usable specific responses.



Warning:

Time is not counsel's friend in ESI discovery. Desirable data can disappear, or the opposition may gather the data and process it in ways that are not desirable to the requesting party. Negotiations in this area need to begin *early*, which is why the Discovery Act and Rule of Court were amended to require these discussion earlier in the discovery process. To obtain the information early enough to be useful, the ESI Systems PMK deposition is the best option.

Advantages of taking a PMK pre-discovery deposition include:

- The information will be available quickly--within a few weeks of noticing the deposition.
- The PMK designee will, by definition, have the information desired and must answer counsel's questions.
- The information will be firsthand information, direct from the knowledgeable witness without a lot of pre-screening or reinterpretation by counsel.
- The PMK generally provides actual answers to pointed deposition questions, as opposed to the boilerplate that usually results from interrogatories.



22 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

III. TAKING A PRE-DISCOVERY ESI SYSTEMS PMK DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.21

AUTHOR: Diane E. Barry, Esq.

5A.21 Drafting Pre-Discovery ESI Systems PMK Deposition Notice: Reasonable Particularity Requirement.

The ESI Systems PMK deposition notice must "describe with reasonable particularity the matters on which examination is requested." This is an area that stymies most counsel, as most are not proficient in computer systems architecture. A basic form for this purpose is provided with this chapter. This form should be reviewed with a technical consultant or expert to tailor it to the needs of the particular matter, and the likely systems for the kind of defendant and litigation matter [CCP § 2025.230].

► **Cross References:**

Drafting a PMK deposition notice, 5A.13

Serving a PMK deposition notice, 5A.14

Form:

See 5A.47, Deposition Notice for ESI Systems PMK Deposition.



23 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

III. TAKING A PRE-DISCOVERY ESI SYSTEMS PMK DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.22

AUTHOR: Diane E. Barry, Esq.

5A.22 Technical Assistance With Preparation and Deposition Is Essential.

The purpose of a pre-discovery PMK deposition is to get sufficient information to draft specific discovery requests. Knowledge of the technical aspects of ESI is essential and is beyond the expertise of most attorneys. For this reason, it is strongly suggested that counsel obtain the assistance of a technical expert early in the process to assist with deposition preparation.



Warning--Bring Technical Expert to Deposition:

The technical expert should also accompany counsel to the deposition itself. A common problem for counsel in this kind of deposition is that counsel prepares well, and understands the questions, but the witness speaks a foreign language (technical IT terminology) and counsel fails to fully understand the answers. *This is too expensive an endeavor to come away with less than the full information needed.* It is much less expensive to take the technical resource to the deposition than it is to leave without the information needed.



24 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

III. TAKING A PRE-DISCOVERY ESI SYSTEMS PMK DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.23

AUTHOR: Diane E. Barry, Esq.

5A.23 Preparing to Take a Pre-Discovery ESI Systems Deposition.

5A.23[1] Counsel Should Prepare a Deposition Outline. Counsel should prepare an outline of the matters that will be inquired about during the PMK deposition. Because the deposition will explore technical areas, it should be prepared in conjunction with counsel's technical expert.

The form in 5A.49 is a general checklist of the areas that should be covered at a pre-discovery PMK deposition. The questions obviously will need to be tailored to the specific context of the litigation.

Examples:

- If the litigation is a marital dissolution action, the computer of an errant spouse will be of particular interest, while corporate e-mail probably will be of much less interest. Counsel working on such a matter could cut back on or eliminate the corporate e-mail server questions.
- If the system of interest is antiquated and/or arcane, such as a homegrown self-programmed system for tracking inventory, the checklist would need to be substantially revised and augmented in order to obtain usable information for that system.



Strategic Point:

When considering the checklist and a particular matter, remember that the goal is to come away with a complete list of the ESI available. From this list, counsel will pick those items that are of interest and that should be transformed into written discovery requests.

5A.23[2] Counsel Should Prepare to Question PMK on Both Organization's ESI and Key Individuals' ESI.

5A.23[2][a] General Categories of ESI Important to Litigation. At the deposition, there are two general areas

for questioning, as there are two general categories of ESI that counsel need to be informed about [*Zubulake v. UBS Warburg* (SDNY 2004) 220 FRD 212] :

- ESI created by individual custodians, or "key players."
- ESI created and kept by the organization itself.

Form:

See 5A.49, Checklist for Taking Pre-Discovery IT Systems PMK Deposition.

5A.23[2][b] ESI Created and Maintained by "Key Players." "Key players" have been defined as "those employees likely to have relevant information" [*Zubulake v. UBS Warburg* (SDNY 2004) 220 FRD. 212, 218] . The list of key players usually starts with the persons who were personally involved in the core facts of the litigation, and branches out to more peripheral players as counsel sees fit.

ESI created by key players generally consists of the ordinary e-files that people create in the ordinary course of a business day--word processing documents, e-mails, PowerPoints, Excel spreadsheets, contacts books, journals, etc.

For each such person, counsel needs to know the following [see *Cal. Rules of Ct, Rule 3.724(8)*]:

- What machines the person used during the relevant time frame.
- What kinds of software the person regularly used.
- What data the person regularly created.
- Where that data was and is stored.
- What kinds of removable storage media the person used regularly.
- What (if anything) was done to backup, archive or delete their data.

5A.23[2][c] ESI Maintained by the Organization. Counsel also needs to be informed about the organization's archives and information stores. This kind of information is used and maintained by the enterprise as a whole, rather than being "owned" by a particular individual. This type of information typically includes such things as:

- The organization's Human Resources database.
- The organization's accounting system.
- The organization's e-mail servers.
- Departmental file shares.

The first step is for counsel to sketch out for the PMK the kinds of information that the particular lawsuit requires:

- What kinds of ESI does this organization create in those categories?
- Where does the organization keep this kind of ESI?

- During the relevant time frame, what format was it in?

Example:

An organization's e-mail currently is in a MS Exchange Server, but they used to use LotusNotes, and migrated the e-mail from Lotus to MS in 2004.

If there is more than one system during the time frame, ask all questions twice--about each system.

More detailed areas for questioning along these lines are provided in Form 5A.49.

5A.23[3] Counsel Should Inquire Regarding Document Retention Policies and Practices. The organization may have policies or practices that affect the individual and/or organizational information stores. If possible, counsel should obtain copies of any written document retention policies prior to the deposition. If not, counsel should request that the PMK bring them to the deposition as part of the document request stated in the PMK notice.

Form:

See 5A.47, Deposition Notice for ESI Systems PMK Deposition; 5A.49, Checklist for Taking Pre-Discovery IT Systems PMK Deposition.



Cross Reference:

General discussion of the creation of organizational document retention and destruction policies, see Ch. 16, Establishing Best Practices Regarding Electronically Stored Information.



Strategic Points:

- The key point with respect to document retention and destruction policies is that that a party organization has a duty to identify and preserve relevant ESI. Thus, counsel should determine if the organization has suspended all relevant document and ESI destruction procedures to protect relevant ESI.
- Additionally, document retention policies list the kinds of information the organization has, and the default time periods for retaining such information. Counsel should determine what desirable ESI is listed, the retention period for such ESI. What is available and from what time frames?

Example:

If counsel desires accounting information, the document retention policy will show that the organization generates and keeps that kind of information. It would also show that the retention period for such information is perhaps seven years. If the organization has been following its policy, finding information from 10 years prior may be a challenge.

- Finally, even if the organization has a written policy, counsel should determine if the organization actually has been following its policy. During the PMK deposition, counsel should test the organization's commitment to its stated policy. Was it followed? How does the PMK know? Was it ever audited? What proof of these facts is available? If there were noted holdouts--people who regularly didn't comply--counsel might wish to look at their documents first. They might have more.

5A.23[4] Counsel Should Inquire Regarding Backup Tapes. The goal in a PMK deposition with respect to backup tapes (and other backup media) is to find out what systems were backed up, how often, what time period is represented in the backups for each system, what utility (program) was used to create the backups, what format they are

in (maybe more than one during a relevant time frame), and where they are now. Counsel should determine if they are labeled in any helpful way, showing what system was backed up and what time period the tape pertains to.

Many organizations do not have a well thought-out archival plan. Historic ESI usually is available only from backup tapes. Backup tapes are a "crisis variety" of storage rather than a real archive. Files are stuffed onto a tape, with an eye towards getting as much data as possible onto each expensive tape, rather than with an eye towards neat and quick retrieval.



Strategic Point:

The usual cycle for backup tapes in large organizations is incremental daily backups, replaced at the end of a week by a full backup, and the weeklies replaced by another full backup created at the end of a month. This means that at the end of a year, there are 12 full backups for a particular system. There also tend to be multiple tapes in a particular backup set--perhaps eight tapes required to backup a particular server.

Form:

See 5A.49, Checklist for Taking Pre-Discovery IT Systems PMK Deposition.



25 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

III. TAKING A PRE-DISCOVERY ESI SYSTEMS PMK DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.24

AUTHOR: Diane E. Barry, Esq.

5A.24 Counsel Should Use Results of PMK Deposition to Draft ESI Discovery Demands.

Once the ESI menu has been created through a successful PMK deposition, counsel should be in possession of a listing of all relevant ESI, where it is currently stored, in what format it is currently stored, and any issues the opposing party believes will impede or otherwise affect production. From this list, counsel should consider what is actually desirable, and frame e-discovery demands on that basis.

Example--Focusing Direct Discovery Demands Based on PMK Deposition:

If the PMK explained that most of the e-mails from the relevant time frame are on the corporate e-mail backup tapes and are unlikely to be on the current corporate e-mail servers, the information should be demanded from backup tapes first. Or, based on the PMK deposition, counsel may conclude, for example, that the Human Resources database does not sound fruitful, but the HR departmental network share sounds much more promising. Armed with this kind of information on where the organization actually keeps its information, counsel can issue direct discovery demands.

➡ Cross Reference:

Drafting e-discovery demands, see Ch. 6, Demanding Production of Electronically Stored Information in California Court.



26 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

IV. TAKING A PMK DEPOSITION DURING DISCOVERY--DEPOSING PMK REGARDING A PARTICULAR ESI SYSTEM

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.25

AUTHOR: Diane E. Barry, Esq.

5A.25 CHECKLIST: Taking a PMK Deposition During Discovery--Deposing PMK Regarding a Particular ESI System

☐ Obtain a technical expert or other technical consultant to assist in the following:

- ☐ Assessing adequacy of any proffered ESI systems information.
- ☐ Assessing completeness of ESI productions.
- ☐ Assist with ESI System PMK deposition notice (preparing or attacking).
- ☐ Assist with ESI System PMK Deposition preparation (taking or defending).

Discussion:

See 5A.27[2], 5A.22

☐ Determine if information important to counsel's case is located in a complex ESI system.

Discussion:

See 5A.26

☐ Determine if way in which opponent used system is question of sufficient importance to merit incurring costs of a deposition.

Discussion:

See 5A.18-5A.20

- ☐ Would counsel's experts prefer direct access to data in its original form to run their queries and analysis?

Discussion:

See 5A.29

- ☐ Determine if system in question is complex enough that over-the-counter manuals and tutorial aids are not sufficient to provide instruction required to make efficient use of system.

Discussion:

See 5A.28

- ☐ If information is necessary and worth the cost, prepare and serve ESI systems PMK deposition notice.

Authority:

CCP §§ 2025.220, 2025.230, 2025.240

Discussion:

See 5A.27

- ☐ Calendar time to prepare deposition notice with assistance from technical consultant.

Authority:

CCP §§ 2025.220, 2025.230, 2025.240

Discussion:

See 5A.27, 5A.28, 5A.30s

- ☐ Calendar time to prepare for deposition with assistance from technical consultant.

Authority:

CCP §§ 2025.220, 2025.230, 2025.240

Discussion:

See 5A.31



27 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

IV. TAKING A PMK DEPOSITION DURING DISCOVERY--DEPOSING PMK REGARDING A PARTICULAR ESI SYSTEM

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.26

AUTHOR: Diane E. Barry, Esq.

5A.26 Objective and Strategy.

In the course of discovery it may become apparent that counsel needs information about a particular operating system beyond that obtained in the meet and confer process or other discovery conducted to that point in the action. This situation differs from the one addressed in 5A.16 et seq. in that it is not predicated on an across-the-board lack of cooperation by the opponent, but rather a necessity to acquire additional information on a specific aspect of the opponent's ESI system as discovery progresses and counsel's information needs become clearer. In this type of deposition, the focus is on a particular system or aspect of ESI storage, as opposed to the opponent's ESI systems in general. Because the goals are more specific, the approach to this type of PMK deposition should be specific as well.

Examples--Deposition Seeking Information Regarding a Specific ESI System:

- In *J.B. Hunt Transp., Inc. v. Adams* (ED Mich 2007) 2007 US Dist LEXIS 17577, one of plaintiff's witnesses testified that certain records had already been destroyed, while their website indicated that the records existed. Defendant noticed a FRCP Rule 30(b)(6) deposition requesting both the production of a PMK regarding the organization's mainframe system, and that the PMK bring the mainframe to the deposition or, in the alternative, agree to hold the deposition at a place where the mainframe could be accessed. The court denied plaintiff's motion for a protective order on the grounds that the information was relevant and the defendant's offer to take the deposition at a place where the mainframe could be accessed rendered it not burdensome.
- In *In re Pharmatrak, Inc. Privacy Litig.* (1st Cir 2003) 329 F3d 9, 17, Internet users sued defendant computer services company, alleging that one of its services collected their personal information without permission, in violation of the Electronic Communications Privacy Act of 1986 (ECPA). Prior to bringing a motion for summary judgment, plaintiffs requested, and the court granted, the taking of two FRCP Rule 30(b)(6) depositions to determine how the software service worked--specifically, what information was extracted, captured, and passed to its client's computers.
- In *Aviation Data v. AMEX Travel Related Svcs* (2007) 152 CA4th 1522, 62 CR3d 396, defendant

credit card company represented that as part of a settlement of a class action, it would make certain changes to the way it tracked specific kinds of expenses. A tentative settlement was reached, and several plaintiffs' representatives objected to the settlement. The court opened discovery as to all aspects of the settlement and objections. When the objecting plaintiffs took the deposition of AMEX's lead programmer, he testified regarding how the changes were made--that they had been made for business reasons that did not relate to the lawsuit, and predated the suit and all settlement efforts. As a result, the court refused to approve the settlement on the grounds that the credit card company had substantially misrepresented the benefits that the settlement would bring to the specified class.



28 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

IV. TAKING A PMK DEPOSITION DURING DISCOVERY--DEPOSING PMK REGARDING A PARTICULAR ESI SYSTEM

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.27

AUTHOR: Diane E. Barry, Esq.

5A.27 Counsel Must Frame Specific Questions in Deposition Notice.

5A.27[1] Counsel Must Determine Goals of Deposition. An ESI Systems PMK deposition on a specific system seeks to answer two kinds of questions:

- First, how did the organization use this system?
- Second, how can counsel use this system to generate or locate information required to prove the case?

5A.27[2] Deposition Notice Must Be Drafted to Comply With Reasonable Particularity Requirement. The deposition notice is required to specify with reasonable particularity the areas for questioning [CCP § 2025.230]. For this kind of deposition, sample forms are not particularly useful because the information needed by counsel and counsel's experts about a particular ESI system is both case specific and system specific.

Form:

Form 5A.47, Deposition Notice for ESI Systems PMK Deposition, is a general deposition notice. It will need to be revised by counsel and counsel's technical experts to provide adequate notice regarding what is desired as to the target ESI system.

Strategic Point--Participation of Technical Experts:



Whoever will be using the information from the system--usually counsel's technical expert, who should have experience dealing with the kind of system (database, accounting, human resources, and so on)--should assist in drafting the notice and creating the deposition outline.

The general types of issues to be considered in drafting the deposition notice for this type of PMK deposition are:

- What kinds of information are counsel and counsel's technical experts hoping will be in the system?
- What kind of information or reports would they like to get out of the system?
- What information do they need for their analysis?



Cross Reference:

Discussion of reasonable particularity requirement, see *5A.13[5][a]*.



29 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

IV. TAKING A PMK DEPOSITION DURING DISCOVERY--DEPOSING PMK REGARDING A PARTICULAR ESI SYSTEM

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.28

AUTHOR: Diane E. Barry, Esq.

5A.28 Counsel Should Consider Including Document Request in Notice.

A PMK deposition notice may require that the PMK bring specified documents or categories of documents to the deposition [CCP §§ 2025.230, 2025.220, 2025.480; *Evid Code* § 771; *International Ins. Co. v. Montrose Chemical Corp.* (1991) 231 CA3d 1367, 1372-1373, 282 CR 783 (*Evid Code* § 771 requirement to produce documents used to refresh memory of witness applies to depositions); *Maldonado v. Superior Court* (2001) 94 CA4th 1390, 1397, 115 CR2d 137 (court erred by denying plaintiff's motion to compel where PMK failed to bring all requested documents)].

The notice should at least request all documents that were used to inform and refresh the recollection of the PMK. Counsel also should consider requesting:

- All user and system administrator manuals and training materials that pertain to the systems described in the notice.
- All corporate document retention policies and procedures that were in force during the relevant time frame and that affected the particular system.
- Any documents detailing backup policies and procedures that pertained to the systems described in the notice during the relevant time frame.



30 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

IV. TAKING A PMK DEPOSITION DURING DISCOVERY--DEPOSING PMK REGARDING A PARTICULAR ESI SYSTEM

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.29

AUTHOR: Diane E. Barry, Esq.

5A.29 Counsel May Take Deposition at Place Where System Can Be Demonstrated.

If counsel or counsel's technical consultants have questions about the operation or contents of a particular system, counsel may ask that the witness "bring" with them the ability to access the systems during the deposition. The offices of the party organization are usually the best place for such a demonstration, although current technology will often permit a demonstration through internet or other remote computer connection.

A PMK deposition may be noticed to be taken at the deponent's principal executive or business office in California, or such other suitable place for demonstrating the target systems as opposing counsel will agree [*CCP* § 2025.250; see *J.B. Hunt Transp., Inc. v. Adams* (ED Mich 2007) 2007 US Dist LEXIS 17577 (court upheld right to deposition noticed at place of mainframe computer so that workings of the system could be demonstrated)]. If there is no suitable office in California, and the opposing party will not agree, the noticing party may make a motion to hold the deposition at a place more distant, such as the corporate headquarters, wherever they are, outside California.



Cross Reference:

Permissible places for taking deposition of organization, see 5A.11.



Strategic Points:

- This is an aggressive but not unheard of use of the PMK document production provisions. Counsel who tries this approach should be prepared for a motion for a protective order and/or a motion for sanctions for discovery abuse on the grounds that a discovery vehicle is being used in a manner not authorized or in a manner that abuses or harasses. In addition, if the motion to move the deposition out of state is denied, the court is required to impose sanctions, unless it finds that the losing party acted with substantial justification, or sanctions would be otherwise unjust [*CCP* §§ 2023.010(c), 2023.020 2025.250, 2025.260, 2030.010].

- If the matter has been assigned to a discovery referee, or to special master for discovery, counsel might consider sounding them out on this subject informally, as part of discovery status conferences, before issuing such a notice.



31 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

IV. TAKING A PMK DEPOSITION DURING DISCOVERY--DEPOSING PMK REGARDING A PARTICULAR
ESI SYSTEM

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.30

AUTHOR: Diane E. Barry, Esq.

5A.30 Counsel May Take Experts to Deposition.

The purposes of this kind of deposition are to learn how to use the system in question and/or to analyze how the organization used the system. Counsel should bring to the deposition the technical expert who assisted in drafting the discovery demand or who will be using the data obtained at the deposition. The deponent's answers may bring up unanticipated questions for the expert, and may suggest additional questions that are apparent to the expert but might not be apparent to counsel. Having a technical expert attend will make sure that all such questions are answered appropriately, fully, and completely.



32 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

IV. TAKING A PMK DEPOSITION DURING DISCOVERY--DEPOSING PMK REGARDING A PARTICULAR ESI SYSTEM

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.31

AUTHOR: Diane E. Barry, Esq.

5A.31 Counsel Should Prepare Checklist for Taking Deposition.

As with other types of depositions, counsel should develop a checklist of information to be elicited at the deposition. Because this information is system-specific, this publication does not contain a deposition checklist form for this particular type of PMK deposition. Generally, counsel taking this kind of deposition will want to establish at least the following on the deposition record:

- The qualifications of the PMK regarding the system.
- Review document request that accompanied the deposition notice:
 - What documents has the witness brought and what are they?
 - Did the PMK look personally?
 - Where did he/she look?
 - Who did he/she speak to?
 - If categories are missing, what was done to search for documents in that category? Where would he/she look? Who would he/she speak to?
- The basic history of the system at the organization:
 - Is the system commercially available software; was it customized; did the organization design the system itself?
 - When was the system introduced?
 - What functions does the system perform at the organization?

- What did it replace; how were these functions performed at the organization prior to introduction of this system?
- Does it have functionality that the organization chooses not to use, or for which the organization uses other software/approaches?
- Who was the administrator for this system during the relevant time frame?
- If the system contains time-sensitive information (employee files, accounting records, and so on), what time frame is represented in the active system currently in use by the organization (that is, how far back does the active information go)?
- Is there historical system information available (e.g., old archived versions of this system)?
- How can desired information or reports be retrieved from this system (demonstration if the system is available; detailed description if it is not)?
- Provide samples of reports/documents that are of interest:
 - Could sample document be created from this system?
 - How (demonstration if the system is available; detailed description if it is not)?
- If essential questions were unanswered, does PMK know of anyone who could answer these questions?
 - Who would he/she speak to?
 - Has he/she spoken with those persons--why or why not?



33 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

IV. TAKING A PMK DEPOSITION DURING DISCOVERY--DEPOSING PMK REGARDING A PARTICULAR ESI SYSTEM

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.32

AUTHOR: Diane E. Barry, Esq.

5A.32 Counsel May Pursue Further Options With Respect to Unanswered Questions.

If the PMK provided by the organization is unable to answer all questions in the noticed areas, counsel has two options [see *Maldonado v. Superior Court* (2001) 94 CA4th 1390, 1397, 115 CR2d 137 (discussion of organization's duty to conduct a reasonable investigation and prepare the PMK; PMK was questioned about what they did personally to investigate); *Marker v. Union Fidelity Life Ins. Co.* (MDNC 1989) 125 FRD 121 (inability to answer questions can be treated as refusal to answer); *Great American Ins. Co. of NY v. Vegas Construction Co.* (D NV 2008), 2008 U.S. Dist. LEXIS 108488 (inability to answer most questions is tantamount to non-appearance at deposition)]:

- First, the organization is now bound by the PMK's answer. The PMK's testimony is the organization's testimony. Therefore, if the PMK(s) did not know, the corporation does not know, and counsel can attempt to block later information that negates the answer provided--if the organization had information on this topic, it was required to provide it at the PMK deposition.
- Second, if the non-answer is not acceptable, counsel can bring a motion to compel further testimony or attendance at the deposition by someone who *can* answer. In order to win this kind of motion, it is necessary to lay a foundation, at the deposition or otherwise that the information is available, and the organization did not make it available through its PMK as required. To this end, if essential questions are unanswered, counsel should ask the PMK designee on the record what was done to investigate--what did the PMK do, what is the PMK aware was done, who did the PMK speak to speak to in ascertaining what was done, and where did the organization search for documents.

➤ Cross Reference:

Motion to compel further testimony, see *Ch. 12, Obtaining or Opposing Motion to Compel*, 12.13 et seq.; see also *Matthew Bender(R) Practice Guide: California Civil Discovery*, *Ch. 6, Oral Depositions in California*, 6.44 et seq.



34 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

V. TAKING A POST-DISCOVERY PMK DEPOSITION--DEPOSING PMK REGARDING ESI DISCOVERY
RESPONSES; POSITIONING FOR SANCTIONS

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.33

AUTHOR: Diane E. Barry, Esq.

**5A.33 CHECKLIST: Taking a Post-Discovery PMK Deposition--Deposing PMK Regarding ESI Discovery
Responses; Positioning for Sanctions**

- ☐ Obtain a technical expert or other technical consultant to assist in:
- ☐ Assessing adequacy of any proffered ESI systems information.
 - ☐ Assessing completeness of ESI productions.
 - ☐ Assist with ESI system PMK deposition notice (preparing or attacking).
 - ☐ Assist with ESI system PMK deposition preparation (taking or defending).

Discussion:

See 5A.36

- ☐ Have opposing party and/or counsel engaged in discovery abuse which strongly indicates that not all relevant ESI has been produced, such as:
- ☐ Outright refusal to produce relevant ESI.
 - ☐ Refusal or unreasonable delay to meet and confer regarding ESI claimed to be not reasonably accessible.

- ☐ ESI discovery production deadlines missed repeatedly or without adequate explanation.
- ☐ Quantity of e-mails and other ESI actually produced seems inadequate.
- ☐ E-mails and ESI produced indicate existence of other ESI that was not produced.
- ☐ Opposing counsel or party certifies an inadequate or otherwise incomplete production.
- ☐ Opposing counsel or party fails, refuses, or delays certification of ESI production.

Authority:*CCP §§ 2023.010, 2023.030***Discussion:**

See 5A.34, 5A.35

- ☐ Has counsel engaged in and documented a reasonable meet and confer effort regarding any inadequate ESI production or other ESI related discovery abuses?

Authority:*CCP §§ 2025.220, 2025.230, 2025.240***Discussion:**

See 5A.19

- ☐ What sanctions are available for type of ESI related discovery abuse at issue?

Authority:*CCP § 2023.030***Discussion:**

See 5A.37[1], [2]

- ☐ Are available sanctions worth costs of pursuing PMK deposition, followed by motion for sanctions?

- ☐ Will they add value to case?

Discussion:

See 5A.34

- ☐ Calendar time to prepare deposition notice with assistance from technical consultant.

Authority:*CCP §§ 2025.220, 2025.230, 2025.240***Discussion:**

See 5A.36, see also 5A.13

- ☐ Calendar time to prepare for deposition with assistance from technical consultant.

Authority:

CCP §§ 2025.220, 2025.230, 2025.240

Discussion:

See 5A.336, 5A.37



35 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

V. TAKING A POST-DISCOVERY PMK DEPOSITION--DEPOSING PMK REGARDING ESI DISCOVERY RESPONSES; POSITIONING FOR SANCTIONS

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.34

AUTHOR: Diane E. Barry, Esq.

5A.34 Objective and Strategy.

The objective of a post-discovery ESI PMK deposition is to document prior e-discovery abuses. This deposition is usually taken towards the end of discovery, or thereafter, and seeks to establish the factual grounds required to punish the other side for discovery-related abuses. It typically is taken after a lack of response, an incomplete response, or a pattern of lack of cooperation in the e-discovery process. The ultimate goal is to make a motion to compel and obtain evidentiary sanctions or the striking of pleadings or defenses. Lesser sanctions are also available, and may also make this effort worthwhile.

In some matters, e-discovery goes so awry that a party's ability to reasonably prepare the case is impacted negatively and severely. This is when e-discovery failures reach the level of discovery abuse. If the other side has recklessly or purposefully failed to preserve and/or produce relevant ESI, has been continually slow and/or late in ESI production, or if it appears that significant and relevant ESI is missing from the production--missing time periods, sources, and/or topics--counsel should consider bringing a motion to compel production, or for sanctions.

An ESI systems PMK deposition can be strong and compelling evidence to support a motion to compel and/or for sanctions. This kind of ESI systems deposition examines the offending party's ESI discovery response process, such as the following:

- Was the opposing party's litigation hold process adequate?
- Did the opponent move quickly and reasonably to preserve all relevant ESI?
- Was all ESI properly collected using appropriate forensic tools and procedures?
- Was all relevant ESI properly produced within a reasonable time frame?
- Did the opposing party sign discovery certifications at a time when there was no reasonable basis for doing so?

Examples--Sanctions Based Upon ESI Discovery Abuse:

■ In a patent infringement case, plaintiff failed to produce more than 46,000 relevant e-mails and e-documents that had been requested in discovery, and which plaintiff had agreed to produce. When plaintiffs' counsel became aware of the failure during final trial preparation, they chose not to bring the matter to the attention of the court or opposing counsel. When the discrepancies were discovered at trial, counsel told the court that the e-mails had been discovered, but had not been produced as they were not responsive to any prior discovery request. The court found that the plaintiff's outside attorneys had either intentionally or recklessly assisted their client in committing a tremendous discovery violation through poor e-discovery practices. Monetary sanctions were issued against the client and against the attorneys, both in-house counsel and outside counsel. The court also referred the attorneys to the State Bar for potential discipline for violations of Rules 5-200 and 5-220 [*Qualcomm Inc. v. Broadcom Corp.* (SD Cal 2008) 2008 US Dist LEXIS 911, *64, vacated in part, *Qualcomm Inc. v. Broadcom Corp.* (SD Cal 2008) 2008 U.S. Dist. LEXIS 16897] .

■ Plaintiffs' failure to impose a litigation hold when they began tracking related litigation, or at least once the instant suit was filed and transferred to the particular federal district, constituted gross negligence. The failure to preserve ESI for years, and to contact and follow up with key players, was likewise grossly negligent. The court ordered a charge to the jury that it would be permitted to presume that the missing documents were relevant, and would have assisted defendants' case. The defendants were also invited to submit a fee application, the charges from which would be allocated among the culpable plaintiffs [*University of Montreal Pension Plan v. Banc of America Securities* (SDNY 2010) 2010 US Dist. LEXIS 1839] .

➡ **Cross References:**

Seeking sanctions for noncompliance with e-discovery, see Ch. 13, Seeking or Opposing Sanctions for Noncompliance.

Seeking motion to compel in an e-discovery matter, see Ch. 12, Obtaining or Opposing Motion to compel.



36 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

V. TAKING A POST-DISCOVERY PMK DEPOSITION--DEPOSING PMK REGARDING ESI DISCOVERY RESPONSES; POSITIONING FOR SANCTIONS

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.35

AUTHOR: Diane E. Barry, Esq.

5A.35 Deposition Usually Is Contentious and Aggressive.

This is a very aggressive and contentious type of PMK deposition. Both sides know that the purpose of this deposition is to show that the target did a horrible job of e-discovery, and to make a case for extreme and costly sanctions. The deponent often is not happy to be in the chair giving this deposition. If mistakes had not been made, it is unlikely that he or she would be here. In addition, the deponent is often from the technical staff of the target organization. This means that on top of being the one who needs to explain how mistakes were made and how poor judgment was used, other work is piling up on the PMK's desk as the deposition progresses. These facts often result in an unhappy and passive-aggressive deponent who is unwilling to provide cooperative responses to pointed questions.



Strategic Point:

The nature and circumstances of this type of deposition make meticulous preparation essential.



37 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

V. TAKING A POST-DISCOVERY PMK DEPOSITION--DEPOSING PMK REGARDING ESI DISCOVERY RESPONSES; POSITIONING FOR SANCTIONS

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.36

AUTHOR: Diane E. Barry, Esq.

5A.36 Technical Assistance Throughout Entire Process Is Essential.

Since counsel is preparing to take the deposition of a reluctant and probably embittered technical person, it is strongly advisable that counsel obtain the assistance of a technical consultant to assist with the deposition preparation, and at the deposition itself. The technical consultant can assist in preparation, and should also attend the deposition and assist in the questioning.



Warning:

In this type of deposition, it is very important for counsel to have technical support during the deposition itself. Preparation will go a long way to help counsel understand the questions he or she is asking, but counsel also needs to understand the answers the PMK gives, determine whether or not they are responsive, and follow up appropriately. Although counsel often grimace at the additional costs imposed by taking technical support to the deposition, the costs of the deposition can rise even more steeply without such assistance. Sometimes the accurate response is technical, and it can take half an hour or more for the deponent to explain the answer to the understanding of non-technical counsel. If the consultant lets counsel know that the technical answer given was sufficient, and is understood by the consultant, even if it is not fully clear to counsel, counsel can move on to use precious deposition time on another topic. The consultant can explain later. The presence of a technical person also is usually sufficient to prevent the deponent from playing games at the deposition, and from wasting deposition time with technical doublespeak or long-winded answers to simple questions.



Strategic Point:

If in-person attendance by the technical consultant is not possible, often it is possible to arrange for the consultant to attend by phone and send "notes" to counsel by e-mail or chat.



38 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

V. TAKING A POST-DISCOVERY PMK DEPOSITION--DEPOSING PMK REGARDING ESI DISCOVERY RESPONSES; POSITIONING FOR SANCTIONS

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.37

AUTHOR: Diane E. Barry, Esq.

5A.37 Counsel Should Prepare Checklist for Taking Deposition.

5A.37[1] Counsel Should First Review Available Types of Sanctions. In preparation for this deposition, counsel should review the discovery sanctions framework used in civil matters, and determine what types of sanctions are potentially available in the action.

A full panoply of sanctions is available for misuse of the discovery process [*see CCP §§ 2023.020, 2023.030*]. A court may impose sanctions to the extent authorized by the chapter governing any particular discovery method or any other provision of the discovery title [*CCP § 2023.030*]. Sanctions for misuse of the discovery process can include any of the following [*CCP §§ 2023.020, 2023.030*]:

- Monetary sanctions.
- Payment of attorneys' fees and costs.
- Establishment of facts without need for further proof.
- Issue sanctions (deeming that certain issues have been determined against an offending party).
- Barring the introduction of evidence.
- Striking of pleadings or defenses.
- Staying or dismissing the action in part or in whole.
- Terminating an action in favor of the aggrieved party.
- Treating the discovery abuse as contempt of court.

**Strategic Point:**

Counsel should carefully consider what sanctions are likely to be available in light of what can be elicited at the deposition, and consider whether those sanctions are worth the cost of this deposition and the subsequent sanctions motion.

**Cross Reference:**

Discussion of discovery sanctions, see *Ch. 13, Seeking or Opposing Sanctions for Non-Compliance*, 13.03 et seq.; see also Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 3, *Sanctions*.

5A.37[2] Counsel Should Review Statutory List of Acts Constituting Misuse of Discovery Process. The facts counsel would like to elicit at the deposition are those that will support sanctions by showing misuse of the discovery process. Accordingly, counsel should review the statutory grounds for misuse of discovery and tailor the discovery checklist towards eliciting information that will prove those grounds. Misuse of the discovery process includes, but is not limited to, the following [CCP § 2023.010(a)-(i)]:

- Persisting, over objection and without substantial justification, in an attempt to obtain information or evidence that is beyond the scope of permissible discovery.
- Using a discovery method in a manner that does not comply with its specified procedures.
- Employing a discovery method in a manner or to an extent that causes unwarranted annoyance, embarrassment, or oppression, or undue burden and expense.
- Failing to respond or to submit to an authorized method of discovery.
- Making, without substantial justification, an unmeritorious objection to discovery.
- Making an evasive response to discovery.
- Disobeying a court order to provide discovery.
- Making or opposing, unsuccessfully and without substantial justification, a motion to compel or to limit discovery.
- Failing to confer in person, by telephone, or by letter with an opposing party or attorney in a reasonable and good faith attempt to resolve informally any dispute concerning discovery, if the section governing a particular discovery motion requires the filing of a declaration stating facts showing that an attempt at informal resolution has been made.

5A.37[3] Checklist Should Walk Deponent Through Prior Steps Taken in E-Discovery. The basic steps for ESI production are: identify, preserve, collect, process, review, produce. The deposition questions should seek detailed information on the following points:

- What did the opposition do (or fail to do) for each of these steps?
- With the benefit of 20-20 hindsight, what went wrong, and why wasn't better process used?
- Who made these decisions and why?

The deposition should walk the PMK through the opponent's process from the time when the opponent knew (or should have known) that litigation was reasonably imminent.



Strategic Point:

A good place to start is with the basic IT custodian deposition checklist, to elicit what kinds of ESI existed if the target organization had been looking properly. Counsel should then follow the opponent's e-discovery process, and the effect that these missteps had on the case.

Form:

General PMK deposition checklist, see 5A.49, Checklist for Taking Pre-Discovery IT Systems PMK Deposition.

PMK ESI deposition notice, see 5A.47, Deposition Notice for ESI Systems PMK Deposition, parts A and B. Part B of this form is specifically applicable to the type of PMK deposition discussed in this part.



39 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice
VI. DEFENDING AN ESI-RELATED PMK DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.38

AUTHOR: Diane E. Barry, Esq.

5A.38 CHECKLIST: Defending an ESI-Related PMK Deposition.

- ☐ Upon receipt of deposition notice, consider informally contacting counsel for noticing party to discuss provision of requested information through means other than a formal deposition.

Authority:

*CCP §§ 2023.010(c), 2023.020; Parker v. Wolters Kluwer United States, Inc. (2007)
149 CA4th 285, 57 CR3d 18*

Discussion:

See 5A.48

Form:

See 5A.48 (checklist for meet and confer with opposing counsel regarding IT systems)

- ☐ Obtain technical expert or other technical consultant to assist in:
- ☐ Assessing specificity of PMK deposition notice.
 - ☐ Assist with PMK deposition preparation.
- ☐ Examine PMK deposition notice and determine if it is specific enough to permit:
- ☐ Identification of a person or persons who can respond on behalf of corporation or other entity.
 - ☐ Education of a person to respond to all noticed areas of inquiry on behalf of entity.

- ☐ Taking of a reasonable deposition within reasonable period of time.

Authority:

CCP § 2025.230

Discussion:

See 5A.41

- ☐ If deposition notice attempts to require production of a specific natural person, draft and send formal letter objecting to specification of a natural person, or to notice as void.

Authority:

CCP § 2025.230

Discussion:

See 5A.41[1]

- ☐ If deposition notice does not specify an appropriate place for PMK deposition, draft and send formal letter objecting to specified place.

Authority:

CCP § 2025.250

Discussion:

See 5A.41[4]

Form:

See 5A.48

- ☐ If deposition notice is overbroad, or time for preparation is too short, meet and confer with opposing counsel to attempt to narrow scope of notice or lengthen time.

Authority:

CCP §§ 205A.020, 2023.010(c), 2023.020, 2025.230; Parker v. Wolters Kluwer United States, Inc. (2007) 149 CA4th 285, 57 CR3d 18

Discussion:

See 5A.41[5]

Form:

See 5A.48

- ☐ If counsel will not agree to narrow scope of PMK deposition notice topics, consider bringing motion for protective order to narrow scope, or to avoid deposition altogether on grounds that it is an abuse of discovery as stated.

Authority:

CCP §§ 205A.020, 2023.010(c), 2023.020, 2025.230; Parker v. Wolters Kluwer United States, Inc. (2007) 149 CA4th 285, 57 CR3d 18

Discussion:

See 5A.42

☐ If meet and confer efforts are fruitless, consider bringing motion for protective order to do one or more of the following:

- ☐ Narrow scope of deposition;
- ☐ Lengthen time before deposition;
- ☐ Stay deposition completely;
- ☐ Request that information in question be obtained through other discovery methods; and/or
- ☐ Seek sanctions for discovery abuse for failure to meet and confer, and for using a discovery vehicle in manner that harasses.

Authority:*CCP § 2023.010; 2025.410; 2025.420***Discussion:**

See 5A.42

☐ If deposition is to go forward, contact client to discuss choosing one or more appropriate PMK(s).

Authority:

CCP § 2025.230; Maldonado v. Superior Court (2002) 94 CA4th 1390, 1395-1397, 115 CR2d 137
(discussing corporate litigant's duties in selecting and educating a PMK for deposition)

Discussion:

See 5A.44

Form:

See 5A.50

☐ Arrange with client for whatever investigation that will be necessary to adequately prepare PMK(s).

Discussion:

See 5A.44

Form:

See 5A.50

☐ Schedule time with PMK(s) to prepare him/her/them for deposition.

Authority:

CCP § 2025.230; Maldonado v. Superior Court (2002) 94 CA4th 1390, 1395-1397, 115 CR2d 137

(discussing corporate litigant's duties in selecting and educating a PMK for deposition)

Discussion:

See 5A.45

Form:

See 5A.50

☐ Calendar time to prepare for deposition with assistance from technical consultant.

Authority:

CCP §§ 2025.220, 2025.230, 2025.240

Discussion:

See 5A.45[3]

Form:

See 5A.50



40 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

VI. DEFENDING AN ESI-RELATED PMK DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.39

AUTHOR: Diane E. Barry, Esq.

5A.39 Objective and Strategy.

A PMK deposition is not a desirable discovery vehicle from the point of view of the organization to be deposed. The organization must conduct an expensive investigation and send a representative, whose testimony is binding upon the organization, to testify on its behalf at an expensive deposition. If possible, it is to be avoided. If it cannot be avoided, it must be managed. Defense of a PMK deposition involves the following basic steps:

- Determine whether the PMK notice contain any fatal flaws.
- Determine if the deposition would amount to a misuse of discovery [see *CCP § 2023.010*]-in other words, harassment. If so, meet and confer and, if necessary, bring a motion for a protective order, or to stay the deposition, or to quash the deposition notice.
- Meet and confer to determine if the deposition can be avoided by offering to provide the information another way.
- If the deposition cannot be avoided, attempt to meet and confer to determine if the scope of the deposition notice can be narrowed so that preparation will be smoother and the deposition shorter.
- If meet and confer fails, again consider bringing a motion for a protective order, or to stay the deposition, or to quash the deposition notice.
- If the deposition cannot be avoided, conduct a reasonable investigation to gather the organization's knowledge on this subject, and simultaneously identify a reasonable PMK or series of PMKs and educate them on matters likely to be addressed at the deposition.
- Prepare the designated deponent(s).
- Attend and defend the deposition.



Warning:

The PMK deposition notice sets out the duties of the target organization. Unless the notice is re-negotiated or voided, the organization must identify, educate and produce a witness or witnesses who can answer questions regarding the noticed subjects. Further, the PMK's testimony will be binding upon the organization *for all purposes*. A PMK's testimony is not simply the PMK's personal testimony--it is the testimony of the organization [*see CCP § 2025.230*]. This means that if the witness cannot answer, the organization will be deemed not to have answered the question. If the witness says he/she doesn't know, the organization doesn't know. If the witness cannot answer, a court can rule that the organization failed to attend the deposition; that is, no one with knowledge attended the deposition. Conflicting information provided later can be barred from use. There are a multitude of unpleasant outcomes that can result from the poor selection or preparation of a PMK.



41 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

VI. DEFENDING AN ESI-RELATED PMK DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.40

AUTHOR: Diane E. Barry, Esq.

5A.40 Calendar Response Period Immediately Upon Receipt of Deposition Notice.

5A.40[1] Written Objections to Deposition Notice Must Be Filed No Later Than Three Calendar Days Prior to Deposition. Any objections to the deposition notice be made in writing no later than three calendar days prior to the deposition, and must be followed quickly with a motion to stay or quash the deposition [*CCP* §§ 2025.230, 2025.410 (objections must be served at least three calendar days prior to deposition noticed, and must be followed by a motion to stay or quash)].



Warning--Proceed Quickly.

If the deposition notice provides a short time for preparation (for example, two weeks notice), time is short to renegotiate a more reasonable deposition and still meet the requirements for a motion to stay or quash [*CCP* §§ 2025.230, 2025.410]. Counsel needs to initiate this process right away.

5A.40[2] Time Extension Should Be Obtained Immediately if Necessary for Adequate Preparation. If the receiving party needs more time to identify and reasonably prepared a witness to respond to a long or complex list of designated topics, counsel should immediately meet and confer to extend the time, followed if necessary with a motion to extend time.

Gaining at least one extension of time is not usually a problem, as the repercussions to a party organization for producing a poorly prepared PMK are unpleasant. This is an important process; the organization should be given sufficient time to take the responsibility seriously and identify, educate and produce a reasonable PMK [*CCP* § 2025.270].



42 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice
VI. DEFENDING AN ESI-RELATED PMK DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.41

AUTHOR: Diane E. Barry, Esq.

5A.41 Attacking the PMK Notice.

5A.41[1] Counsel Should Examine and Resolve Any Problems With Deposition Notice. Counsel's first line of defense is to examine the notice. If there are problems with the notice, they must be addressed immediately. Most particularly, *they must be resolved prior to the deposition itself*. If problems with the notice are not addressed within a reasonable time of receiving the notice, they will be deemed accepted and the scope of the deposition is as stated in the notice [see *CCP §2025.410(a)*]. If the deposition begins without an agreed renegotiation of the terms of the notice, the notice stands as stated and the organization is responsible for the subject matter, etc., in the notice as stated.



Strategic Point--Dealing With Notice Problems.

If counsel finds problems with the deposition notice, the usual methods apply: counsel should first attempt to meet and confer, and if that effort fails, bring a motion for a protective order [*CCP §§ 2025.230* (notice of the deposition of an organization), *2025.280* (effect of a deposition notice), *2025.410* (objections must be served at least three calendar days prior to deposition noticed, and must be followed by a motion to stay or quash), *2025.450* (failure to comply with deposition notice), *2025.520* (use of deposition as evidence); *Maldonado v. Superior Court (2nd Dist 2002) 94 CA4th 1390, 1395-1397, 115 CR2d 137* (discussing corporate litigant's duties in selecting and educating a PMK for deposition)].

5A.41[2] Deposition Notice May Not Identify a Natural Person. It is a common error for noticing parties to attempt to name a particular person to be produced as the PMK. This is a fatal error in a PMK deposition notice.

CCP § 2025.230 specifically states that the PMK deposition notice must be directed to the *organization*. The target organization has both the duty and the privilege of naming its own [*CCP § 2025.230*], who will be providing testimony on behalf of the target organization. If a PMK notice purports to name a particular natural person, it is not a PMK deposition notice. Thus, if the issuing party truly desires to take the deposition of the organization's person most knowledgeable on a particular subject or subjects, the notice must be reissued to state the deposition of the target organization only [see *CCP §§ 2025.220* (deposition of a natural person), *2025.230* (deposition of an organization)].

**Strategic Points:**

- If the issuing party truly desires to take the deposition of the specified person, the notice must be reissued to notice the deposition of the specified natural person.
- If the target organization needs a bit more time to identify and educate its PMK, requiring that the notice be reissued (as opposed to agreeing on amendments) usually re-sets the deposition date further out and provides the target organization with a little additional time.

5A.41[3] Deposition Notice Must Describe Scope of Examination With "Reasonable Particularity." The PMK deposition notice must describe with reasonable particularity the matters on which examination is requested [CCP § 2025.230]. Upon receipt of a PMK deposition notice, counsel should determine whether the notice meets this requirement; in other words, whether it is specific enough to identify what information the organization needs to make available; whether it permits identification of a PMK witness or witnesses, and whether the list of requested information short enough to permit a deposition of a reasonable length within the time specified. Specifically, counsel should consider the following questions:

- Can the organization identify a proper witness or witnesses?
- Does the notice describe particular systems or particular practices and protocols of the organization for examination?
- Does the notice name persons whose systems are of interest?
- Does the notice specify a relevant time period?
- With a bit of investigation, can materials be gathered to inform a witness, and in the amount of time given prior to the stated deposition date?

If the answer to any of these questions is "no," counsel will need to take immediate action to address and resolve these issues [CCP §§ 2025.230 (notice of the deposition of an organization); *Maldonado v. Superior Court* (2002) 94 CA4th 1390, 1395-1397, 115 CR2d 137 (discussing corporate litigant's duties in selecting and educating a PMK for deposition)].

5A.41[4] Place of Deposition Must Be One Authorized by Statute. The deposition of an organization must be taken in specified locations, usually within a certain distance of the organization's principal place of business in California [CCP § 2025.250]. Failure to specify a location authorized by statute or agreed on by the parties is a basis for objection to the notice [see CCP § 2025.410(a) (service of written objections)].

**Cross Reference:**

Locations where statute authorizes PMK deposition to be taken, see 5A.11.

5A.41[5] Counsel May Seek to Meet and Confer Regarding Notice Flaws. It is always appropriate to meet and confer with opposing counsel to settle discovery problems. The notice of a PMK deposition is a matter of sufficient importance that law and motion may well be required if notice flaws cannot be resolved. Issued to be considered include [CCP §§ 2025.230, 2025.250]:

- For scope problems, can the scope be narrowed or the number of subjects reduced? Counsel should not simply object, but should propose an acceptable and reasonable restatement of the scope.
- Is the site of the deposition improper? If so, what would be acceptable?
- If the notice names a natural person, ask the opponent to reissue the notice stating a proper witness designation.

Similar approaches may be taken to other issues arising from the PMK notice.



Strategic Points:

- An additional purpose of the meet and confer attempt is to appropriately position the matter for judicial resolution if it becomes necessary to do so. This is a strong possibility in this area of the law. Counsel should draft pointed meet and confer letters.
- *Start early and move quickly.* The time frame in many cases will not allow for a drawn-out meet and confer process.



Cross Reference:

Time frame for filing formal objections to deposition notice, 5A.40.

- In addition to resolving notice problems, the meet and confer process itself may stretch out the timing of the deposition sufficiently to permit reasonable identification and preparation of a proper designee, even if nothing else is accomplished.
- Failure to meet and confer, even without any other discovery abuses, is a sufficient basis for imposition of monetary sanction [*Parker v. Wolters Kluwer United States, Inc.* (2007) 149 CA4th 285, 294, 57 CR3d 18] .



43 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice
VI. DEFENDING AN ESI-RELATED PMK DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.42

AUTHOR: Diane E. Barry, Esq.

5A.42 Counsel May File Motions to Stay, Quash, or for a Protective Order.

5A.42[1] Counsel May Seek These Remedies If Meet and Confer Is Unsuccessful. If the noticing party refuses to conduct the deposition in a reasonable manner, and meet and confer on these points does not bear fruit, counsel should be prepared to follow up with a motion to stay or quash the deposition, or for a protective order as to particular information or demands.

Consider:

Counsel should be open-minded about what remedy will best serve the interests of the matter. Keep in mind that the party issuing the notice is entitled to discovery on these points, and to take a deposition to obtain that discovery. The duty of counsel for the target organization is to make sure that the discovery is conducted in a reasonable and orderly fashion, designed to produce reliable evidence.

Counsel should tailor the remedy requested to the type of problem:

- If the scope of discovery in the notice is unreasonable, counsel should move for a protective order and ask the court to order a reasonable scope.
- If the time is not sufficient to permit reasonable identification, education and production of a PMK, counsel should ask the court to stay the deposition until a later date.
- If the list of topics is very long, counsel should move for a protective order and ask for a time limit; for example, any questions not covered in five days need not be answered.



Strategic Point:

If the demanded information, or most of it, was already given at the early meeting of counsel, or if the party has been working diligently to obtain and communicate the desired information with opposing counsel, consider asking for a protective order to bar the deposition completely [*CCP* §2025.420;

Nicholas v. Wyndham Int'l, Inc., (4th Cir 2004) 373 F3d 537 (third-party ESI custodian deposition quashed as plaintiffs were apparently complying with their discovery obligations and deposition seemed cumulative and burdensome under circumstances)].



Cross References:

Protective orders in e-discovery, see Ch. 11, Seeking or Opposing a Protective Order.

Objecting to conduct of oral deposition, see *Matthew Bender(R) Practice Guide: California Civil Discovery*, Ch. 6, *Oral Depositions in California*, 6.36 et seq.

Motion to stay deposition or quash deposition notice, see *Matthew Bender(R) Practice Guide: California Civil Discovery*, Ch. 6, *Oral Depositions in California*, 6.26.

5A.42[2] Motion to Stay and Quash a Deposition Notice Provides a Temporary Halt. If there are errors or irregularities in a deposition notice, the receiving party may move for an order to stay the taking of the deposition and quashing the deposition notice [CCP § 2025.410(c)].



Timing:

In order to bring this motion, at least three business days prior to the deposition date, counsel must personally serve the noticing party with written objection listing the errors and irregularities in the deposition notice.

Personal service must be made in compliance with CCP § 1011. This written objection must be quickly followed with filing the motion to stay and quash the deposition notice [CCP § 2025.410(b)].

The motion to stay and quash must be accompanied by a meet and confer declaration as specified in CCP § 2016.040. [CCP § 2025.410(c)]. Upon filing the notice, the taking of the deposition is stayed, pending determination of the motion [CCP § 2025.410(c)].



Strategic Point--Motion to Quash Provides Only Temporary Relief:

If granted, a motion to stay and quash stops the deposition, but does not bar the noticing party from issuing a new deposition notice--one that does not contain the old errors and irregularities--and proceeding with the deposition. If counsels desire to avoid the deposition entirely, the proper choice is a motion for a protective order [see 5A.43[3]].



Strategic Point--Electing Not to Attend Deposition:

A slightly riskier tactic is set out in CCP § 2025.410(b). CCP § 2025.410(b) states that after personal service of the written objections as described above, the party can elect not to attend the noticed deposition. If the objections are judged to be valid, there is no penalty for failure to attend the deposition. This also puts the onus on the noticing counsel either to renegotiate the notice, or to bring a motion to compel attendance at the deposition, or for sanctions for skipping the deposition. However, counsel must bear in mind that if the later adjudication does *not* hold that the objections are valid, sanctions and penalties which accompany failure to attend the deposition will follow.

5A.42[3] Motion For a Protective Order Provides a Permanent Halt. Any deponent may bring a motion for a protective order before, during, or even after a deposition [CCP § 2025.420(a)]. If the court finds that the deposition

constitutes unwarranted annoyance, embarrassment, or oppression, it can order that the deposition not be taken at all, that it be taken at a different time or place, or that it be taken only under specified conditions [*CCP* § 2025.420(b); *Nicholas v. Wyndham Int'l, Inc.*, (4th Cir 2004) 373 F3d 537 (third-party ESI custodian deposition quashed as plaintiffs were apparently complying with their discovery obligations and deposition seemed cumulative and burdensome under the circumstances)].

**Strategic Point:**

For PMK depositions, a motion for a protective order can let a party avoid the deposition altogether, or can gain the court's assistance in revising the conditions of the deposition such as the place, the scope, the number of days permitted, or other conditions for taking the deposition. Unlike a motion to stay and quash, once the court grants a motion for a protective order, the court's revisions cannot be evaded simply by issuing a new deposition notice.



44 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

VI. DEFENDING AN ESI-RELATED PMK DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.43

AUTHOR: Diane E. Barry, Esq.

5A.43 Organization Has Duty to Conduct Reasonable Investigation.

On receipt of a PMK deposition demand, the target organization is required to conduct a reasonable investigation into the subject matter in order to inform itself on the specified topics, and then to share the fruits of this investigation for the education of the PMK. This investigation should include at least the following [*CCP § 2025.230*; see *Maldonado v. Superior Court* (2002) 94 CA4th 1390, 1395-1397, 115 CR2d 137 (discussing corporate litigant's duty to conduct a reasonable investigation to inform its PMK, which should have included former employees and documents)]:

- Present employees.
- Past employees.
- The organization's current and past written policies and manuals that address the topic in whole or in part.
- Relevant documents and ESI in current use.
- Archival papers and ESI.

The form in 5A.50 is a detailed checklist for preparing a PMK deponent. This checklist illustrates the information that typically should be included in the organization's investigation, and which will be necessary to properly prepare the PMK deponent for the deposition. It details who to talk to, what kinds of questions to ask, and the kinds of considerations when assessing a particular person for designation as the PMK.



45 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice
VI. DEFENDING AN ESI-RELATED PMK DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.44

AUTHOR: Diane E. Barry, Esq.

5A.44 Organization Must Select Suitable PMK(s).

5A.44[1] Organization Designates Its Own PMK(s). The organization, not the opponent, selects its own PMK(s) [CCP § 2025.230]. The organization is directed to "designate and produce at the deposition those of its officers, directors, managing agents, employees, or agents" who are "most qualified" to testify on its behalf regarding the listed areas of inquiry [CCP § 2025.230].



Cross Reference:

Additional discussion of PMK selection, see 5A.12.

5A.44[2] PMK Need Not Have Pre-Existing Knowledge of Subject Matter. The statute does not require that the target organization produce any particular kind of person, let alone someone who has pre-existing personal knowledge on the named topics. The target organization can select *anyone* as its agent for this deposition, and then educate them on the subjects for the deposition, as long as they are "most qualified to testify on [the organization's] behalf as to those matters to the extent of any information known or reasonably available to the deponent" at the time of the deposition [CCP § 2025.230].



Strategic Point:

In response to the PMK deposition notice, organizations tend to select and produce current or former employees who worked in the areas of inquiry, because those persons already have at least some knowledge of the deposition subject areas. This is not required, however, and is not necessarily the best use of the organization's opportunity to designate a PMK.

Consider:

- The subject matter of this kind of deposition is often corporate practices that involved many persons, often across long time frames. It is unusual for all information of this kind to be known to a single

person.

Example:

It is unlikely a single person will be familiar an organization's e-mail archiving practices from 1990 to the present.

- As case law interprets *CCP § 2025.320*, the target organization is required to educate its PMK designee regarding things the organization "knows" but which were not within the personal knowledge of the PMK designee [see *Maldonado v. Superior Court (2002) 94 CA4th 1390, 1395-1397, 115 CR2d 137*].

- The designee and the organization are required to conduct a reasonable investigation--speaking to past and present employees, looking through relevant documents, and so on--so that the designee can provide all testimony available to the organization on a subject. This negates the idea that the PMK must have personal pre-existing knowledge of the subjects upon which he or she may testify.

- A PMK deposition is the deposition of *an organization*. The knowledge of an organization on a particular topic is likely to be an accumulation of knowledge dispersed across time and the organization, stored in persons, papers, and ESI. *CCP § 2025.230* allows the noticing party to demand that this dispersal of information be accumulated in one person who will present it in a neat and tidy testimonial package for the issuing party. This role does not require personal knowledge of the subject matter, so long as a firm understanding is acquired and presented on the deposition date.

5A.44[3] Designated PMK Should Be Good Spokesperson for Organization. The organization has, in effect, the opportunity to pick its own "perfect witness." In deciding who to designate as potential PMKs, the following should be considered:

- Who would make a good spokesperson for the organization?
- Who is smart, technologically savvy, and personable on the stand?
- Who can present the noticed topic(s) in an organized and understandable way?
- Who can learn everything they need to learn in the amount of time given?
- Who is interested in answering the questions for the organization, who will not be frustrated because work is piling up on their desk as the deposition goes forward?



Strategic Point--Frequent Litigants:

If the client is a serial litigant, and expects this kind of PMK deposition regularly, it should consider identifying a good PMK on regular topics in advance, and keeping the person "on tap." A similar approach is to keep a set of PMK educational materials on regular topics that are updated regularly. Both approaches relieve the stress of attempting to select and educate the PMK in a short period of time prior to a noticed deposition. Either the PMK is already ready, and needs only to be brought up to date, or the educational materials are ready and the PMK can start in to study immediately, rather than wait until after the reasonable investigation has been conducted.



46 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

VI. DEFENDING AN ESI-RELATED PMK DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.45

AUTHOR: Diane E. Barry, Esq.

5A.45 Organization Must Educate PMK.

5A.45[1] PMK Is Required to Know All Information Reasonably Available to Organization. The organization may not simply designate a person with personal knowledge and rely upon that personal knowledge. The PMK must be educated so that all information reasonably available to the organization is provided [*see CCP § 2025.230*].



Warning:

The PMK will be presenting the organization's testimony, and the PMK's testimony will be binding upon the organization for all purposes. For this reason, it is also in the organization's best interests to reasonably inform its PMK [*CCP § 2025.230; see Maldonado v. Superior Court (2002) 94 CA4th 1390, 1395-1397, 115 CR2d 137*].

5A.45[2] Checklist for Selecting and Educating PMK. The form in 5A.50 is a detailed checklist of factors to consider in selecting a PMK and the information that the PMK is likely to need in order to be properly prepared for a PMK deposition. Counsel should review that list and modify it to reflect the contents of the particular PMK deposition demand.



Trap:

Be careful of showing the PMK any privileged items. As with other witnesses, anything that "refreshed" the witness's recollection must be produced upon request [*see Evid Code § 771*]. Since most documents shown to a PMK educated them--"refreshed" their corporate recollection--most documents used to prepare a PMK are discoverable.

5A.45[3] Counsel Should Allow Sufficient Preparation Time. Preparation for a PMK deposition is usually more time-intensive than preparation for the depositions of a natural person. It takes time to conduct the reasonable investigation. It takes time to synthesize and prepare materials for the education of the PMK. It takes time to identify and educate a proper PMK. ESI-related PMK depositions are usually on technical and complex topics and take even more time to prepare.

**Strategic Points:**

- Counsel should work hard to be ready, but should not let the noticing party push the organization into a deposition before the PMK is ready. If necessary, counsel should bring a motion to stay a PMK deposition to gain more time for reasonable preparation of the PMK.
- If time is short and the topics truly long, counsel should consider breaking up the topic into manageable chunks, and using more than one PMK for a topic.
- In some cases it may be helpful to designate different PMKs to testify as to different time frames.

Example:

One PMK may be designated to testify regarding or archival practices of the organization's East Coast office e-mail during 1995 to 2000, another for 2000 to 2004, another for its West Coast office during 1995 to 2000, and so forth.

**Cross Reference:**

Motion to stay deposition, see *Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 6, Oral Depositions in California, 6.26*



47 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice
VI. DEFENDING AN ESI-RELATED PMK DEPOSITION

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.46

AUTHOR: Diane E. Barry, Esq.

5A.46 Deposition Procedure.

5A.46[1] Normal Deposition Procedures Apply. Normal deposition procedures, including objections, apply at a PMK deposition.



Cross Reference:

Discussion of general deposition procedures, see Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 6, Oral Depositions in California.

5A.46[2] Counsel Should Object to Questions Beyond Scope of Deposition Notice. If a question asks for information beyond the scope of the subjects outlined in the deposition notice, counsel should object on the record. If a question is beyond the scope of the topics in the notice, it is not clear whether the question can be barred [see Strategic Point *below*]. However, whether or not the question is answered, if objections are made on the record counsel has laid a proper foundation showing that the corporation should not be bound by the answer; that is, that the corporation did not provide testimony on this point because it was not requested.



Strategic Point--Objecting to Questions Beyond Scope:

In federal courts, the circuits are divided as to whether or not a PMK witness can be asked questions that are outside the scope of the deposition notice [compare *King v. Pratt & Whitney (SD FLA 1995) 161 FRD 475* (questions outside scope of notice not barred) with *Paparelli v. Prudential Ins. Co. (D MASS 1985) 108 FRD 727* (questions limited to subject matter of notice)]. The author was unable to find any California case directly on point. It is probably best not to stop the deposition if only a few questions are outside the scope. Instead, counsel should object clearly on the record and attempt to bar or reclassify the answers at a later date. If the notice sets out the testimony that will be sought on behalf of the corporation, answers outside the scope ought not to be held to be the testimony of the corporation. If the deposition strays well outside the limits of the deposition notice, counsel may choose instead to bar the questions and direct the witness not to answer.



48 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice
VII. FORMS

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.47

AUTHOR: Diane E. Barry, Esq.

5A.47 Deposition Notice for ESI Systems PMK Deposition.

Deposition Notice for ESI Systems PMK Deposition.

SUPERIOR COURT OF CALIFORNIA,
COUNTY OF _____

_____ [name],	)	
Plaintiff,	)	
vs.	)	NOTICE OF TAKING ORAL DEPOSITION OF
XYZ Corporation, Inc.	)	PERSON MOST KNOWLEDGEABLE REGARD-
Defendant.	)	ING ESI SYSTEMS [AND FOR PRODUCTION OF
	)	ESI WRITINGS OR OTHER TANGIBLE THINGS]
	)	

To _____ [list all parties or attorneys for parties who have appeared in the action]:

PLEASE TAKE NOTICE that _____ [specify party, e.g., plaintiff] _____ [name]
will take the deposition, on oral examination, of XYZ Corporation, Inc. The deposition will be taken on
_____ [date], commencing at _____ [time], at
_____ [address where deposition will be taken].

NOTICE IS FURTHER GIVEN that the matters on which examination is requested are as follows:

[For a pre-discovery ESI systems PMK deposition, use Part A below only; delete Part B. For a post-discovery ESI
discovery PMK deposition, use both Part A and Part B.]

A. With respect to Defendant XYZ Corporation's ESI systems:

1. A description of the computer systems used by each XYZ Corporation employee specified in Attachment 1 to this deposition notice, during the time period of _____ [date] through and including the present. The description must include hardware, software, peripherals, network connectivity, and whether any of these items have been upgraded, changed or replaced during the time period _____ [date] through and including the present. The description must include all of the following:

- a. Desktop computers.
- b. Laptop/portable computers.
- c. Personal digital assistants (PDAs).
- d. Telephones (land lines and cellular).
- e. Other similar personal electronic devices.
- f. Individually assigned network storage areas.

2. A description of the XYZ e-mail system used during the time frame _____ [date] through _____ [the present or specify other date]. The description must include specification of the system hardware and software as well as the protocols for storage and deletion of e-mails from the corporate e-mail servers and/or the personal work systems of any of the XYZ corporate employees specified in Attachment 1 to this deposition notice. The description must also include whether there have been updates, changes, or replacements made to system hardware or software components, or to storage and protocols, during the time frame _____ [date] through _____ [the present or specify other date].

3. The identity of all persons who are or were responsible for managing and maintaining the YOUR information technology infrastructure during the time period _____ [date] through and including the present, and a general description of the duties of each such person. This infrastructure specifically includes:

- a. Servers and other network storage devices and related peripheral equipment.
- b. Desktop computers.
- c. Portable computers.
- d. Laptop computers.
- e. Personal digital assistants (PDAs).
- f. Telephones.
- g. Other similar electronic devices.

4. A description of and operation of the Internet and intranet connectivity available to each of the XYZ corporate employees specified in Attachment 1 to this deposition notice, during the time frame

_____ [date] through _____ [the present or specify other date].

5. A description of all groups of connected computer systems maintained by YOU and available to the XYZ Corporation employees named in Attachment 1 to this deposition notice, that permit users to share information and transfer data. Please include local area networks (LANs), wide area networks (WANs), client server networks, virtual private networks (VPNs), and storage area networks (SANs), and all equipment, devices components and network resources that establish and maintain the network environment.

6. A description of, including the operation of, all available third-party connectivity between the computer systems and network environment used by YOU, including the type of information that is shared, the manner in which the information is transferred, and the identity of any individuals who have authorization to transfer information into or out of the network environment.

7. A description of the policies and procedures governing the use of all removable media such as CD-ROMs, Zip discs, floppy discs, tape drives, removable hard drives, associated with YOUR computer systems or network from _____ [date] through _____ [the present or specify other date].

8. A description of the policies and procedures used for performing backups on all computer systems, including e-mail systems, and a description of any hardware or software used to perform such backups from _____ [date] through _____ [the present or specify other date].

9. A description of all policies and procedures pertaining to data retention and destruction from _____ [date] through _____ [the present or specify other date], and a description for all hardware and/or software used to facilitate the deletion of data subject to any data retention and destruction policies and procedures.

10. A description of any servers or other network storage devices, desktop computers, portable computers, laptop computers, personal digital assistants (PDAs), telephones, and other similar electronic devices that have had their hard drives reformatted, wiped or replaced from _____ [date] through and including the present.

11. A description of YOUR ESI naming conventions, specifically including file-naming and location-saving conventions, disc or tape labeling conventions.

12. A description of YOUR corporate policies regarding employee use of company computers and data.

[For a post-discovery ESI discovery PMK deposition, include Part B below. Delete Part B for a pre-discovery ESI systems PMK deposition.]

B. With regard to ESI produced in the above-captioned action:

1. The process and means utilized by YOU to identify the ESI considered relevant to the above captioned matter.
2. The process and means utilized by YOU to preserve the ESI considered relevant to the above captioned matter.
3. The process and specific means utilized by YOU to collect the YOU to identify the ESI considered relevant to the

above captioned matter.

4. The process and specific means utilized by YOU to process the ESI considered relevant to the above captioned matter for privilege/responsiveness/relevance review.

[CONTINUE for all ESI discovery PMK depositions]

Pursuant to *Code of Civil Procedure Section 2025.230*, XYZ Corporation, Inc. shall designate and produce at the deposition one or more of its officers, directors, managing agents, employees, or agents who are most qualified to testify on its behalf as to the above-described matters to the extent of any information known or reasonably available to the deponent. It is hereby requested that XYZ Corporation, Inc. provide prompt notification in writing to the undersigned as to the name, address, telephone number, capacity, and job title of each person so designated to testify and the matters on which this person will testify.

[Add if deponent is to produce writings or other tangible things]

NOTICE IS FURTHER GIVEN that the above-described deponent or the person designated by XYZ Corporation, Inc. to testify on its behalf is hereby required to bring and produce at the deposition, at the time and place set out above, the following _____ *[writing(s) and/or (other) tangible thing(s)]*: _____ *[specify with reasonable particularity any materials or category of materials to be produced by deponent]*.

[ADD, if noticing party intends to record deposition using audio or video technology]

NOTICE IS FURTHER GIVEN that _____ *[party noticing deposition, e.g., Plaintiff]* intends to record the testimony at the above-described deposition by _____ *[audio and/or video]* recording, in addition to recording this testimony by the stenographic method.

[ADD, if noticing party intends to record testimony by stenographic method, through instant visual display of testimony]

NOTICE IS FURTHER GIVEN that _____ *[party noticing deposition, e.g., Plaintiff]* intends to record the testimony at the above-described deposition by stenographic method, through instant visual display of testimony.

[CONTINUE]

The deposition will be taken before _____ *[name of deposition officer and descriptive title, if any, or a deposition officer]* who is authorized to administer an oath. If the deposition is not completed on the date set out above, the taking of the deposition will be continued from day to day thereafter, except for Sundays and holidays, at the same place, until completed.

Date: _____

_____ *[firm name, if any]*

By: _____ *[signature]*

_____ *[typed name]*

Attorney for _____

[noticing party's status and name]

The following persons are known to be involved in the subject matter of this litigation or otherwise are likely to have relevant information regarding that subject matter: _____ [*add list of names of known "key players" of entity being deposed*].

NOTES:

Authority:

CCP § 2025.230.

Drafting a PMK Deposition Notice:

See 5A.13, 5A.21, 5A.27.

Service Requirements for PMK Deposition Notice:

See 5A.14.

Attacking a PMK Deposition Notice:

See 5A.41.

Related Checklist for PMK Deposition Preparation:

See 5A.49



49 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice
VII. FORMS

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.48

AUTHOR: Diane E. Barry, Esq.

5A.48 Letter From Deponent's Attorney Proposing Meet and Confer Process to Narrow Scope of PMK Deposition.

Letter From Deponent's Attorney Proposing Meet and Confer Process to Narrow Scope of PMK Deposition.

[*law firm letterhead*]

_____ [*name of opposing party's attorney*]

_____ [*law firm name*]

_____ [*address*]

Re: _____ [*case name*], Case No. _____

Dear Mr/Ms. _____ :

I am writing to open a meet and confer process regarding the deposition of XYZ Corporation currently scheduled for _____ [*date*]. The deposition notice is deficient in several respects. When you have had a chance to review this letter, I would appreciate it if you would contact me so that we can discuss and resolve them in time for this deposition to go forward on the date specified in the notice.

[*Delete any of the following grounds that are inapplicable to the case*]

1. The deposition notice does not describe the matters on which examination is requested with the "reasonable particularity" required by CCP § 2025.230.

CCP § 2025.230 requires that when the deposition of a corporation is noticed, the notice must specify with "reasonable particularity" the subject matter upon which examination is requested. Based upon the specifications in the notice, XYZ Corporation is required to conduct an investigation and then to select and educate a proper Person Most Knowledgeable

to testify on behalf of the corporation on the topics noticed [*Maldonado v. Superior Court (2002) 94 CA4th 1390, 1395-1397, 115 CR2d 137*] .

The list specified in your notice is overbroad, and does not provide sufficient specifics to permit XYZ Corporation to conduct such a process, in that _____ [with input from technical expert if necessary, provide some specifics regarding what is overbroad about the notice topics, what specificity is lacking, and what would the noticing party need to know in order to make a reasonable PMK preparation, e.g., it asks for a PMK as to all IT systems. A broad-based specification of "all IT Systems" is not sufficient to permit reasonable preparation and response. XYZ Corporation is a very large company with more than 5,000 current employees, and the sheer number and complexity of its systems precludes a response to such a general specification. More specificity is required as to what is being requested; for example, are you interested in XYZ Corporation's e-mail system, or its accounting system? In addition, there are different protocols for the information created by individual users, and that created by and kept by the corporation. Furthermore, the notice does not specify a time frame for the information desired. The system XYZ Corporation used for e-mail two years ago is different than what it uses now]. We therefore are unable to understand what your client wishes to know, [and for what time period], and therefore are unable to conduct a reasonable process to investigate, identify, and educate an adequate PMK who can provide testimony to your client.

2. The place notice for the deposition, _____ [specify location named in notice], does not meet the statutory requirements for the place where the deposition of a corporation may be taken.

CCP § 2025.250(b) specifies that the deposition of an organization must be taken in one of two places. Either the specified location must be within 75 miles of XYZ Corporation's principal executive or business office in California, or it must be within the county where the action is pending *and* still be within 150 miles of that office.

The deposition is currently noticed to be taken at _____ [e.g., your offices or other address]. As the principal office for XYZ Corporation is located at _____ [address], the location specified meets neither of the distance criteria set out in *CCP § 2025.250*. The deposition will need to be held at a different location which meets the statutory requirements.

3. The deposition notice notices the deposition of XYZ Corporation, but demands that XYZ Corporation produce a specified natural person as its Person Most Knowledgeable.

The Code of Civil Procedure authorizes depositions of two kinds of persons: natural persons, and entities. The deposition of an entity, in this case a corporation, is authorized by *CCP § 2025.230*. *CCP § 2025.230* specifically authorizes the corporate deponent, in this case XYZ Corporation, to select the most appropriate person to testify on its behalf on the topics noticed. Your client may not compel XYZ Corporation to designate a specific person to testify.

If your client wishes to take the deposition of _____ [name of specific person named in notice], your client will need to issue a deposition notice for a natural person rather than noticing the deposition of XYZ Corporation. If your client prefers to take the deposition of XYZ Corporation on the described topics, you will need to amend the notice to remove the demand that XYZ produce a particular person to testify on those topics.

[Add any additional grounds and CONTINUE]

If you would like to set up a time to meet and confer with me regarding the contents of the deposition notice, with a

view toward reaching a mutually acceptable scope and level of specificity, and the other issues referenced above, so that the deposition of XYZ Corporation may proceed, please contact me by phone, e-mail, or letter at the address indicated above.

Sincerely,

_____ [signature of attorney]

[typed name]

_____ [name of law firm]

NOTES:

Authority:

Cal Rules of Ct, Rules 3.724(8) (e-discovery meet and confer), 3.727(9) (discovery issues in meet and confer and case management conference)

Discussion of Attacking Deficiencies in PMK Deposition Notice:

See 5A.41

Discussion of Using Meet and Confer to Resolve Deposition Issues:

See 5A.19, 5A.41[5]



50 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice

VII. FORMS

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.49

AUTHOR: Diane E. Barry, Esq.

5A.49 Checklist for Taking Pre-Discovery IT Systems PMK Deposition.

I. Document Retention Programs/Practices.

1. Does XYZ Corporation have a written document retention program? If yes, does the program have the following items in writing?

- a. A document retention policy?
- b. A document retention schedule or other document that identifies custodians or persons responsible for carrying out archival and destruction functions?
- c. Has the retention program changed during the relevant time frame?
- d. Request copies of all retention program documents that pertain to the relevant time period. The goal is to obtain copies of all documents that pertain to the time period, and not just the current program.
- e. If the program changed, how did it start, and how did it change over time?

2. Provide deponent with a list of the affected custodians, departments named or described in the PMK deposition notice. If XYZ Corporation did not have an official retention program, are there retention/destruction/backup practices that affected the custodians, and departments listed in the notice? Did any affect the corporate IT group in general?

- a. For each category (custodians, departments, etc.), who is the person who knows the most about what was done for archiving, retention and destruction of ESI during the relevant time period? (Ask deponent "If you were investigating, who would you ask?")

b. Would time period affect deponent's choice of who to talk to for each category; i.e., did the person's identity change over the relevant time period?

3. Has XYZ Corporation taken any steps to identify ESI relevant to this litigation, and to halt destruction or collect the ESI?

a. What steps were taken to identify relevant ESI? Is there documentation of the steps taken and persons notified and/or talked to?

b. What steps were taken to halt destruction? Is there documentation of the steps taken and persons notified and/or talked to?

c. If ESI has been collected, what collection personnel and methods were used?

i. For personnel--name, whether they are in-house or from an outside vendor, title/function, forensic collection qualifications (forensic collection certifications such as EnCe, CISSP, etc.) and essential details of experience in forensic collections.

ii. Methods: what collection tools were used? (Are they recognized in the legal industry as forensically sound, i.e., capable of creating a reliable, forensic quality, bit for bit copy? Drag-and-drop methods do not meet these criteria.)

II. Natural Persons/Key Players.

1. For the natural persons/key players listed in the deposition notice, identify all ESI creation and storage devices to which XYZ Corporation owns or has right of access:

a. Laptops.

b. Office workstation.

c. Home office workstation. (Do they perform work on home computers?)

d. Guest office work stations.

e. PDAs/cell phones.

f. iPod/other MP3 and data storage devices.

g. Removable storage media--floppy discs, thumb drives, CD ROMs, removable hard drives, etc.

2. For each device identified:

a. Has the person changed devices during the relevant time frame? (Has the person been issued a new laptop or PDA?)

b. If yes, what happened to the old machine?

c. Has the device ever been backed up? By corporate IT or by the person, or both?

- d. If the custodial person backs up his or her own device, where are all backups located?
 - e. If the custodial person backs up his or her own device, has anyone informed the person that all backups from the relevant time period cannot be altered or deleted, and must be preserved for the pending litigation? Has anyone communicated a litigation hold request to the person, and, if so, was it written and/or oral?
3. Do any of the persons listed on the notice store information on the corporate network? If yes, where?
4. If the key player's laptop computer were to crash, or be destroyed by an earthquake, would all of the information on the laptop be lost? If no, where would the key player go to retrieve information?

III. Corporation/Enterprise Data.

1. E-mail.

a. System history.

i. What is the current enterprise e-mail system in use? (MS Exchange, Notes/Domino, Groupwise, etc ...)

ii. What version is currently in place?

iii. How long has this system been in use?

iv. What is the system architecture?

1. How many servers are currently in use?

2. How many sites are currently in the enterprise? How are these sites connected (SMTP, POP, native protocols)?

3. Are there offline capabilities for traveling users/laptops?

v. Was there a prior system?

1. What was the prior system?

2. When was it officially retired from service?

3. Was the system migrated and data converted to the new system?

4. Are backups or data files from the old system still available?

b. General.

i. Are there size restrictions on server mailboxes?

1. What are the restrictions?

2. Are there exceptions?

- ii. Are users able to and/or trained on how to create local drive stores for their e-mail?
- iii. Is there an archiving policy in place? If so, what is it? Automated or manual?
- iv. Do users keep mail stores on shared network drives as well as local drives?
- v. Can users forward their e-mail to external accounts?
- vi. Are users issued Blackberries or other PDAs with corporate e-mail connectivity?

2. E-files.

a. System history.

- i. What network operating system(s) are in place (Netware, Windows, UNIX/LINUX, etc.)?
- ii. How long have these systems been in place?
- iii. Are there any processes for archiving or data migration to off-line storage in place?
- iv. Do users have access to a corporate FTP site for file transfers?
 - 1. Is access restricted or is there a general login provided for all users?
 - 2. Is this data backed up along with other network resources?
- v. Were they preceded by a prior system?
 - 1. What was the prior system?
 - 2. When was it officially retired from service?
 - 3. Was the system migrated and data converted to the new system?
 - 4. Are backups or data files from the old system still available?

b. General.

- i. Is there an enterprise document storage policy? What is it?
- ii. Are any document management systems in place (MS SharePoint, IBM/Lotus QuickPlace)?
 - 1. Are these used on a regular basis?
 - 2. Are there retention and revision controls in place?
 - 3. Are these systems included in the enterprise backup plan?
- iii. Is security and administration centralized or distributed (i.e. enterprise domain vs. local domains vs.

workgroups)?

iv. Common configurations.

1. Is there a standard corporate PC configuration? What is it?
2. What systems are in place (Dell, IBM, HP)? Common HD sizes?
3. Are there any non-PC based systems in place (AS/400, Apple, mainframe, proprietary systems)?
4. What common OS is in place on users' local machines?
 - a. OS (Windows, Linux, OS/2)
 - b. Version (XP Pro, XP Home, 2000 Pro, 98, 95)

5. File System (NTFS, FAT32, FAT16)

6. Percentage of employees using each type.

v. Is there any file encryption technology in place on users' machines?

1. Full Drive, Windows EFS, PGP?
2. Does corporate IT have access to de-crypt files without users' knowledge/cooperation?

vi. Are users provided with a network drive share for private use (home drive)?

1. How do these map to servers and physical drives?
2. Are there space restrictions enforced on the home drives?
3. Are there exceptions to these restrictions?

vii. Are users provided with common network drive shares for group use?

1. What are they?
2. How do they map to servers and physical drives?

c. Storage.

i. Are user documents stored on shared network drives and/or local drives? Is there a general tendency towards one location or the other?

ii. Are users able and/or permitted to use USB thumb drives, PDAs, iPods and other removable storage media in conjunction with corporate PCs?

1. Are the cables and/or cradles available to synchronize them with a computer?

2. What brands and models?

3. Do they have removable memory cards?

3. Backup.

a. General.

i. Is there an enterprise backup policy?

1. Is it documented?

2. Can a copy be provided?

ii. Are backups taken on a scheduled basis?

1. How often are full backups taken?

2. How often are differential backups taken?

3. How long are backups retained?

4. Do backups differ for e-mail and e-file systems? How?

iii. Are backups periodically verified for accuracy and restorability?

1. How often?

2. When was this last done?

iv. Is the purpose of the backup for disaster recovery, data retention, or both?

v. What is the backup architecture?

1. What backup software (brand and version) is in use?

2. Is the backup centralized or distributed?

a. If distributed, how many sites?

b. Do all sites use the same software and hardware?

3. Are backups stored locally on-site, centrally on-site, off-site or a combination?

a. What is the policy for tape storage (local, central and off-site)?

b. Are tapes on a rotation? Please explain.

4. What type and size of media are the backups written to (DLT, LTO, multiple, etc)?

b. E-mail.

i. For what time period do backups of the e-mail system currently exist?

1. Are any backups in this time period known to have failed?

c. E-file.

i. For what time period do backups of network shared resources currently exist?

1. Are any backups in this period known to have failed?

ii. Are (none/some/all) user local drives backed up?

1. Is the backup centralized or user controlled?

2. Is this an automated process?

3. What is the primary backup media (USB Drive, tape, Zip, Jaz, network share)?

NOTES.

Preparation of Outline Checklist for PMA Deposition:

See 5A.23, 5A.31, 5A.37

Importance of Technical Assistance in Preparing Checklist:

See 5A.22

Related Form for Demand in PMK Deposition:

See 5A.47



51 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 5A E-Discovery Deposition Practice
VII. FORMS

1-5A MB Practice Guide: CA E-Discovery and Evidence 5A.50

AUTHOR: Diane E. Barry, Esq.

5A.50 Checklist for Preparing PMK Deponent.

A. Assembling Background Information and Documents.

1. Establish that there was a consistent, defined, and defensible methodology to manage the identification, collection, processing, review, and production of electronic data in a systemized manner.
2. Gather appropriate data policies, system profiles, and ESI roadmaps.
3. Analyze the type of litigation the company is typically involved in and identify individuals who have the requisite knowledge to serve as potential PMK deponents.
4. Understand the impact, if any, of using consultants or outside vendors for maintenance and service of computer systems.
5. Consider using an outside expert for specific categories of inquiry.
6. Understand the roles and responsibility the potential PMK deponent has in responding to discovery requests seeking production of electronic documents.
7. Will the potential PMK deponent be a potential fact witness as well?
8. Identify steps taken by deponent to prepare for deposition, including document review.
9. Be careful what is shown the potential PMK deponent in order to avoid privilege waiver.
10. Have a backup PMK deponent.

B. Evaluating Qualifications of a Potential PMK Deponent.

1. Research the complete qualifications of the potential PMK deponent, including educational background and work experience in regard to the categories of discovery likely to be targeted.
2. Examine potential PMK deponent's scope of knowledge of communications or legal strategy.
 - a. Clarify that potential PMK deponent is not holding any privileged information about the case strategy or e-discovery "meet-and-confer" strategy.
 - b. Get list of anyone potential PMK deponent has spoken with about the litigation.
 - c. Read any memos or e-mail or any communications by the witness about it. Find out how to see potential PMK deponent's e-mails on this topic.
3. Examine role of potential PMK deponent in company's e-discovery process.
 - a. All job roles and responsibilities of potential PMK deponent.
 - b. Background, training, education, job history.
 - c. Confirm that potential PMK deponent has no reasons for bias in the instant litigation.
 - d. What was role of potential PMK deponent in matter being litigated?
4. Examine on a preliminary basis--at a high level--the activities of which potential PMK deponent has knowledge.
 - a. What has potential PMK deponent observed, managed, or measured?
 - b. Determine the parameters of his/her role in this e-discovery process.
5. Who else has been involved in this e-discovery effort in any way?
 - a. What are their identities, roles, backgrounds?
 - b. What was their involvement in this process?
 - c. Was it unusual that they were involved?
 - d. Is there a consistent e-discovery team at the company?
 - i. Who is part of that team?
 - ii. Were they all involved?
 - iii. If not, why not?
6. Examine the organization's structure.
 - a. To whom does potential PMK deponent report?
 - b. Who reports to potential PMK deponent?

- c. Same information for all members of the e-discovery team.
- d. Describe the structures in the Legal, IT and IT Security departments.

7. What did potential PMK deponent do to prepare for this deposition?

- a. What did potential PMK deponent look at or do?

C. Understanding Systems, Networks, Storage, Usage Policies, Databases, and E-Mail.

1. Examine general network information and design.

- a. Examine structure of IT/IS department, locations, key IT/IS personnel, duties of system administrators, those responsible for daily operations, maintenance personnel, backup systems.

2. Examine data processing and data storage devices used by the company in the relevant departments and time frames.

- a. What type of backroom hardware is used (mainframes, mini-computers, electronic mail servers, file servers, fax servers, voicemail servers, etc.)?
- b. What workstation hardware, laptop hardware, PDAs/Blackberries, backup systems, optical storage, electronic storage (non-volatile RAM, smart cards, etc.), other office machines (scanners, copiers, voice-mail systems)?
- c. Hard drives for each of these devices and whether they can be accessed.

3. Examine use of outside consultants.

- a. What outside consultants were used?
- b. What did they do?
- c. How frequently and for how long were they used?

4. Layout and design of network, system architecture, file servers, web servers, e-mail servers, group shares, online work spaces, fax servers, SANs and other processing and storage devices.

- a. Network users: numbers, locations, file sharing and storage (including where their e-mail and electronic documents reside).
- b. Legacy systems.
- c. Applications and databases.
 - i. Company policies on installation or use of application software.
 - ii. What software applications are in use, and their business uses (localize to the relevant departments). Notes? Windows? SAP? PeopleSoft? Software apps on desktops, laptops.

Document management systems (finance/accounting, knowledge-workers' needs, office automation systems).

iii. Types of databases in use in relevant groups, individuals responsible for database and software applications.

5. For each database system:

- a. Types of database server systems and client programs in use.
- b. Types of database software used (Oracle, etc.).
- c. Identity of people who run and administer databases including who enters and accesses information.
- d. Description of database access, how standard reports are prepared on a regular basis, how database backup has been modified to comply with e-discovery preservation requests.
- e. Is data ever deleted from databases; are the databases archived offsite?
- f. Has prospective PMK deponent restored any restored data from a backup system or tape?
- g. Is anything password protected or encrypted?
- h. Are passwords and access codes revoked/changed when an employee leaves or moves to a new role in the company?

6. Records management systems and policies.

- a. Description of record management policies/procedures.
- b. Dates deployed.
- c. Education of employees on these policies.
- d. Compliance efforts.
- e. Naming conventions for files.
- f. User data in connection with documents and e-mails.

7. User workstations and laptops.

- a. Networking issues--is home use possible?
- b. Can employees work on personal computers?
- c. Permissions and preferences for user-driven data storage.
- d. Password or encryption protection.

- i. Where does the "unstructured data" go (e.g. user-created Word, Excel, PowerPoint, and other programs)?

8. E-mail.

- a. Describe e-mail system used, administrator and administration personnel. User-directed archiving of e-mails.
- b. Can users access their electronic mail remotely? How?
- c. Are backups made?
- d. Size of permitted e-mail storage and how size limit is enforced.
- e. Deletion policies.
 - i. Whether they relate to inbox only or other folders (e.g. deleted items, sent items, drafts, personal folders).
 - ii. Compliance with deletion policies.
 - iii. Policy exceptions and exception tracking.
 - iv. Size and location of PSTs encountered.
 - v. Are programs used to purge e-mail (e.g., system administrators emptying waste baskets on a schedule)?
 - vi. Are files ever deleted from the e-mail systems?
- f. What other e-mail systems were previously in operation?
 - i. Where is the legacy data?
- g. Are electronic mail passwords routinely changes?
- h. Have any e-mails been restored in the past 12 months?
- i. Are passwords or encrypted files used on any of the e-mail systems?
 - i. If so, how does one access them?

9. Instant messaging. See e-mail above.

10. Voicemail. See e-mail above.

11. When someone leaves the company, what happens to their ESI?

D. Understanding Company's E-Discovery Processes and Procedures.

1. Are there written policies and procedures?
 - a. When were they written, revised, last updated?
 - b. Who has copies?
 - c. Are they posted online?
 - d. Are they privileged?
 - e. Have they been maintained confidentially?
 - f. Do they vary by size or type of litigation?
2. Have they been used on prior and other current litigations? When, what, how?
3. What are the e-discovery policies and procedures?
 - a. Examine in depth, who does what, when, how, and why.

E. History and Status of Current Litigation.

1. What was prospective PMK deponent's earliest communication on this matter?
2. Who has been involved?
3. What is understanding of prospective PMK deponent about the litigation, parties, claims, relevant types of information, potential custodians, timeframe?
4. Was there any oral or written communication about how to handle the preservation of e-mail and electronic evidence? What were they?
5. What were the instructions from company's legal department (privileged)?
 - a. Who in legal department was involved?
 - b. When did they meet, decide?
 - c. Is there anything in writing?
 - d. To whom were legal department's instruction communicated?
 - e. How did potential PMK deponent learn of this?
 - f. Are there e-mails or other evidences of communications or plans (e.g., PowerPoints, Excel spreadsheets, Word documents)?
6. What challenges were perceived as possible with respect to this preservation?
7. How did the preservation go? Details.

8. What steps were taken to prevent any of the ESI from being destroyed or erased before it could be preserved?
- a. What was the method of collection of the ESI?
 - b. What was the approach toward each of following:
 - i. E-mail?
 - ii. Databases?
 - iii. Unstructured data?
 - iv. Other sources of ESI?
 - v. Backup?
 - c. Was there any requirement that newly created data also be preserved?
 - d. Chronology of everything that has taken place up until today with respect to e-discovery on this matter.
 - i. Who was involved?
 - ii. Who did what?
 - iii. How long did it take?
 - iv. What did that cost?
 - e. Was there any documentation memorializing compliance with policies, or decisions taken, with respect to the preservation?
 - i. Did anyone keep notes?
 - ii. Were any tracking applications used?
 - iii. Was there tracking of spending?
 - iv. Did any aspect of these activities stray outside the parameters of the company's e-discovery policies and procedures?
9. Is any relevant ESI that has not yet been collected?
- a. What is it, and why hasn't it been collected?
 - b. What collection plan exists going forward?
10. How would prospective PMK deponent characterize the e-discovery process in this matter to date?

- a. What is different about it from other cases?
 - b. Was it better or worse than usual?
 - c. What made it easy/difficult?
 - d. What could have been handled better?
11. How familiar is prospective PMK deponent with the legal requirements for e-discovery?
- a. What is required for a company's e-discovery processes and procedures to be defensible?
 - b. What about the company's e-discovery processes and procedures make it defensible (e.g., preservation of metadata)?
 - c. What is prospective PMK deponent not sure about?
12. Is prospective PMK deponent aware of the production of ESI in other litigation or legal proceedings at the company?
- a. How were those handled differently?
13. Review sample preservation letter, cover instructions, custodian list, and keywords with prospective PMK deponent.
14. Issues with custodians (e.g., if one is in Europe, what was done with regard to EU data protection and transfer restrictions?)
- a. What sorts of data did prospective PMK deponent collect for each of them?
 - b. What could not be collected?
 - c. Are all the custodians still with the company?
15. Did prospective PMK deponent do testing or sampling with the keywords?
- a. What were the results of that testing and sampling?
 - b. Are there written reports and/or other documentation reflecting those results?
16. How much data was collected?
17. Where is it now?
18. Have all instructions regarding data collection instructions been followed in all ways? If not, how not? Explore.

NOTES.**Discussion of Organization's Duty to Educate PMK Deponent:**

See 5A.45

Selection of an Appropriate PMK Deponent:

See 5A.44



52 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 6 Demanding Production of Electronically Stored Information in California Court

1-6 MB Practice Guide: CA E-Discovery and Evidence 6.syn

§ 6.syn Synopsis to Chapter 6: Demanding Production of Electronically Stored Information in California Court

6.01 Scope.

6.02 Objective and Strategy.

6.03 CHECKLIST: Determining What to Ask for.

6.04 Options and Strategies.

6.05 Party May Obtain Production of Any Electronic Information That Is Within Scope of Discovery.

6.06 Demanding Party Should Consider What Types of Electronically Stored Information to Request.

6.06[1] "Electronically Stored Information" Is Any Information Stored in Electronic Form.

6.06[2] Demanding Party Should Consider What Production Format to Specify In Demand.

6.07 Party May Demand Copy of Electronic Information.

6.07[1] Copy of Information Is Usually Sufficient to Meet Litigation Needs.

6.07[2] Demanding Party Should Consider Whether Data Is Reasonably Accessible.

6.07[2][a] Responding Party May Object or Seek Protective Order.

6.07[2][b] Court May for Good Cause Order Discovery.

6.07[2][c] Court May Allocate Discovery Expenses.

6.08 Party May Demand to Test, Sample, or Inspect Electronic Information.

6.08[1] Testing or Sampling Allows Determination of Whether Information Is Relevant.

6.08[2] Demanding Party May Seek to Inspect Responding Party's Computer System.

6.09 CHECKLIST: Preparing and Making Demand.

6.10 Options and Strategies.

6.11 Production Demand Must Comply With Formal Requirements.

6.11[1] Demand Must Meet Prescribed Format and Content Requirements.

6.11[1][a] Demands Must Be Consecutively Numbered.

6.11[1][b] First Paragraph Must Contain Identifying Information.

6.11[1][c] Each Demand Must Be Separately Identified.

6.11[1][d] Each Demand Must Specify Item or Category of Item Being Demanded.

6.11[1][e] Demand Must Specify Time for Inspection.

6.11[1][f] Demand Must Specify Place for Inspection.

6.11[1][g] Demand Must Specify Type and Manner of Activity Being Demanded.

6.11[1][h] Demand Should Specify Form of Production.

6.11[2] Demand Should Be Tailored to Specific Facts of Case.

6.11[3] Demand Should Not Be Overbroad or Unduly Burdensome.

6.12 Propounding Party Must Serve Demand.

6.12[1] Demand May Be Served Within Times Authorized by Statute.

6.12[2] Copy of Demand Must Be Served on All Other Parties.

6.12[3] Demand Is Not Filed With Court.

6.12[4] Demanding Party Must Retain Original Demand and Response.

6.13 Demanding Party Should Review Response and Production.

6.13[1] Responding Party Must Serve Timely Response.

6.13[2] Counsel Should Determine Whether to Move to Compel Further Response or Compliance With Demand.

6.13[3] Demanding Party Must Promptly Return Privileged Information That Was Inadvertently Produced.

6.14 CHECKLIST: Obtaining Electronic Evidence From Nonparty.

6.15 Options and Strategies.

6.16 Party May Subpoena Electronically Stored Information From Nonparty.

6.16[1] Discovery From Nonparty Is Available If Party Does Not Possess Reliable Evidence.

6.16[2] Subpoena May Require Production of ESI.

6.17 Subpoena for Electronically Stored Information Must Comply With Statutory Requirements.

6.17[1] General and Special Subpoena Requirements Apply to Subpoena for ESI.

6.17[1][a] General Subpoena Rules Apply to ESI.

6.17[1][b] Special Subpoena Requirements Apply to ESI.

6.17[2] Subpoena Is Issued by Clerk of Court or by Counsel.

6.17[3] Subpoena Should Designate ESI and Date of Production.

6.17[4] Subpoenaed Person Must Be Protected From Undue Burden or Expense.

6.17[5] Federal Stored Communications Act Limits Subpoenas to Electronic Communications Services.

6.17[6] Federal Stored Communications Act Governs Third-Party Subpoenas to Social Networking Sites.

6.18 Subpoena Must Be Served.

6.19 Subpoenaed Person Must Comply With or Oppose Subpoena.

6.19[1] Subpoenaed Person May Oppose Subpoena Based on Undue Burden or Expense.

6.19[2] If Subpoenaed Person Does Not Oppose Subpoena, or Opposition Is Overruled, Electronic Information Must Be Produced.

6.19[3] Subpoenaed Person May Be Sanctioned for Noncompliance.

6.19[4] Subpoenaing Party Must Promptly Return Privileged Information That Was Inadvertently Produced.

6.20 Sample Demands for Production of Electronically Stored Information.

6.21 Sample Demand for Inspection.

6.22 Subpoena Duces Tecum (Judicial Council Form SUBP-010).



53 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 6 Demanding Production of Electronically Stored Information in California Court
I. STRATEGY

1-6 MB Practice Guide: CA E-Discovery and Evidence 6.01

6.01 Scope.

This chapter covers:

- Determining what electronic information should be the target of a discovery demand, and whether the demand should be for a copy of the desired information or for inspection of a computer or other storage device [see 6.03-6.08].
- Preparing and making the production demand [see 6.09-6.13; *Forms*: 6.20, 6.21].
- Obtaining electronic evidence from a nonparty [see 6.14-6.19; *Form*: 6.22].

For discussion of the preliminary procedures that should be undertaken prior to filing an e-discovery demand, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference*, 5.03-5.08.

For discussion of the procedures for obtaining or opposing an injunction to preserve electronic evidence pending discovery, see *Ch. 7, Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery*, 7.09-7.15.

For discussion of the procedures for responding to a demand for the production of electronic evidence, see *Ch. 8, Responding to Electronic Discovery Demands in California Court*, 8.12-8.23.

For discussion of the procedures for gathering and producing electronic evidence, see *Ch. 9, Gathering and Producing Electronically Stored Information*.

For discussion of the procedures for opposing a demand for the production of electronic evidence, see *Ch. 10, Opposing Demands for Production of Electronic Evidence in California Court*.

For discussion of the procedures for seeking or opposing a protective order, see *Ch. 11, Seeking or Opposing Protective Order*, 11.03-11.12.

For discussion of the procedures for making or opposing a motion to compel a response or a further response to a

demand for production, or a motion to compel compliance with a demand for production, see Ch. 12, Obtaining or Opposing Motion to Compel.

For discussion of the procedures for seeking or opposing sanctions for noncompliance with production demand, see *Ch. 13, Seeking or Opposing Sanctions for Noncompliance, 13.11-13.15*.

For discussion of the procedures for obtaining production of electronic evidence in foreign jurisdictions, see Ch. 14, Discovery of Electronically Stored Information Residing in Foreign Jurisdictions.

Core Statutes:

CCP §§ 2031.010-2031.050.



54 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 6 Demanding Production of Electronically Stored Information in California Court

I. STRATEGY

*1-6 MB Practice Guide: CA E-Discovery and Evidence 6.02***6.02 Objective and Strategy.**

Early in the litigation, counsel should become familiar with the specific kinds of electronically stored evidence involved in the case, and the manner in which that evidence is maintained, so as to decide which kind of discovery demand will be most effective and efficient.

Early consultations with opposing counsel in good faith will help clarify discovery concerns and help counsel formulate an effective discovery plan [see *Cal Rules Ct, Rule 3.724(8)*]. Counsel may also seek judicial guidance early in the case to avoid problems that may arise concerning preservation and production of electronically stored information [see *Cal Rules Ct, Rule 3.728(13)* (case management order may include orders relating to discovery of electronically stored information)]. This preparation will enable counsel to formulate effective discovery demands that will maximize the benefits and minimize the costs of discovery of electronic information.

**Cross References:**

Discussion of forms in which electronic evidence is maintained, see 6.06; see also Ch. 1, Understanding Electronic Evidence.

Learning about the opposing party's data storage systems, see Ch. 4, *Planning E-Discovery*, 4.09.

Preservation notices and litigation holds, see Ch. 5, *Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferring, and Case Management Conference*, 5.09-5.21.

Discussion of available kinds of discovery demands, see Ch. 6, *Demanding Production of Electronically Stored Information in California Court*, 6.07, 6.08.

**Strategic Point--Reasonable Inquiry:**

Counsel's early consultations with opposing counsel should include inquiries about potential claims of privilege and confidentiality that might be made in response to demands for discovery of electronic information. If possible, counsel and opposing counsel should come to an agreement concerning how privileged and confidential documents will be dealt with in discovery [see *Cal Rules Ct, Rule 3.724(8)(E), (F)*].

 Cross Reference:

Discussion of claims of privilege and confidentiality, see *Ch. 10, Opposing Demands for Production of Electronic Evidence in California Court*, 10.08.

**Strategic Point-Reasonable Diligence:**

Counsel's early consultations with opposing counsel should also include an attempt to arrive at an agreement about how the cost of the production of electronic evidence is to be allocated among the parties [see *Cal Rules Ct, Rule 3.724(8)(G)*].

 Cross References:

Discussion of discovery planning, see *Ch. 4, Planning E-Discovery*, 4.03-4.10. Discussion of meeting and conferring and case management conferences, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferring, and Case Management Conference*, 5.22-5.25.



55 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 6 Demanding Production of Electronically Stored Information in California Court

II. DETERMINING WHAT TO ASK FOR

1-6 MB Practice Guide: CA E-Discovery and Evidence 6.03

6.03 CHECKLIST: Determining What to Ask for.

☐ Determine what information is discoverable.

Authority:

CCP § 2017.010

Discussion:

See 6.05

☐ Review elements of each party's claims and defenses to determine what facts will be relevant at trial.

☐ Consider information that may be possessed by each party and whether such information will be admissible at trial, or is likely to lead to discovery of admissible evidence.

☐ Consider whether any information possessed by another party is subject to claim of privilege or work-product protection.

☐ Determine whether any discoverable information is likely to be maintained or stored in electronic form, considering various types of electronic data and devices that may be possessed by each party.

Discussion:

See 6.06

☐ Determine which form of electronically stored information would be most useful in preparing for trial.

Discussion:

See 6.06

- ☐ Determine whether electronically stored information is reasonably accessible, and if not, whether there is good cause for discovery.

Authority:

CCP §§ 2031.010(a), 2031.060

Discussion:

See 6.07[2]

- ☐ Determine whether to demand copy of electronically stored information, or whether to demand testing or sampling of information.

Authority:

CCP §§ 2031.010(a), 2031.060

Discussion:

See 6.07[1], 6.08[1]

- ☐ Determine whether to demand inspection of other party's computer or other devices containing electronically stored information.

Authority:

Dodge, Warren & Peters Ins. Servs., Inc. v. Riley, 105 CA4th 1414, 1417-1418, 130 CR2d 385

Discussion:

See 6.08[2]



56 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 6 Demanding Production of Electronically Stored Information in California Court
II. DETERMINING WHAT TO ASK FOR

1-6 MB Practice Guide: CA E-Discovery and Evidence 6.04

6.04 Options and Strategies.

Deciding what electronically stored information to seek in discovery is an important step in litigation. Making the right decisions about what information to seek will save time and expense and can contribute to a party's ultimate success in the litigation. An overbroad demand (for example, for "all e-mails sent or received by defendant") may be met with a motion for a protective order [see *CCP § 2031.060*], which increases the cost of the litigation. Even if the responding party complies with an overbroad demand, litigation costs will likely be increased because counsel will need to review the large volume of material produced, with little of it actually being relevant or useful in the litigation [see *Jackson v. City of San Antonio (WD Tex 2006) 2006 US Dist LEXIS 8091, at *4* (production was not impermissible "data dump" because it was responsive to demand, and burden of culling out relevant information was substantially same for both sides)]. On the other hand, a too-narrow demand for production risks missing an opportunity to discover relevant evidence.

Cross References:

Discussion of motion for protective order in response to burdensome production demand, see 6.07[2].

Procedure for obtaining and opposing protective orders, see *Ch. 11, Seeking or Opposing Protective Order, 11.03-11.12*.

Counsel should be familiar with the characteristics of the electronically stored information (e.g., searchability and the existence of metadata) in the form in which it is ordinarily maintained by the responding party (i.e., in its "native" format). Whether counsel will need to have those characteristics preserved in the produced copy of the information, and whether the computers and software available to counsel (or to counsel's expert) can make use of those characteristics, will determine whether a demand for production should specify that the information be produced in a form other than its native format [see *CCP § 2031.030(a)(2)*].

Cross References:

Discussion of forms of electronically stored information, see 6.06, and *Ch. 1, Understanding Electronic Evidence*.

Also important is the decision whether to seek a copy of the desired information or to demand to inspect the computer or device on which the information is stored. If the responding party has indicated (in earlier discovery or at a case management conference or other meeting of counsel) that the desired information has been lost or deleted, counsel may

demand an inspection of the computer or other storage medium, to determine whether the deleted material can be recovered [see *Playboy Enters. v. Welles* (SD Cal 1999) 60 F Supp2d 1050, 1052-1055] .

**Cross References:**

Discussion of demand for copy of electronically stored information, see 6.07[1].

Discussion of demand to inspect computer system, see 6.08[[2].



57 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 6 Demanding Production of Electronically Stored Information in California Court

II. DETERMINING WHAT TO ASK FOR

1-6 MB Practice Guide: CA E-Discovery and Evidence 6.05

6.05 Party May Obtain Production of Any Electronic Information That Is Within Scope of Discovery.

Any party to an action may demand that any other party produce and permit the party making the demand (or someone acting on that party's behalf) to inspect, copy, test, or sample electronically stored any information that is within the scope of discovery and is in the possession, custody, or control of the party on whom the demand is made [CCP § 2031.010(a), (e)].

Electronically stored information is within the scope of discovery if (1) it is not privileged, (2) it is relevant to the subject matter of the pending action or to the determination of any motion in the action, and (3) it is admissible in evidence or appears reasonably calculated to lead to the discovery of admissible evidence [CCP § 2017.010; see CCP § 2031.010(a)]. The information demanded may relate to the claim or defense of the demanding party or of any other party to the action. Additionally, a demanding party may obtain the identity and location of people with knowledge of any discoverable electronic information, including its existence, description, nature, custody, condition, and location [CCP § 2017.010].

Distinguish:

The scope of discovery under California Civil Discovery Act, which authorizes discovery of material that is relevant to the "subject matter involved in the pending action," is broader than the available scope of discovery under the Federal Rules of Civil Procedure [CCP § 2017.010]. The Federal Rules were amended in 2000 to limit the general scope of discovery to matters relevant to "any party's claim or defense"; discovery on material relevant to the "subject matter involved in the action" is available only if ordered by the court for good cause [Fed R Civ P 26(b)(2)].



58 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 6 Demanding Production of Electronically Stored Information in California Court
II. DETERMINING WHAT TO ASK FOR

1-6 MB Practice Guide: CA E-Discovery and Evidence 6.06

6.06 Demanding Party Should Consider What Types of Electronically Stored Information to Request.

6.06[1] "Electronically Stored Information" Is Any Information Stored in Electronic Form. California law broadly defines "electronically stored information" as "information stored in an electronic medium" [CCP § 2016.020(e)]; that is, any medium having "electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities" [CCP § 2016.020(e); see 1.16]. With the continuing emergence of new technologies, it is essential for counsel to understand the types of electronic information (e.g., e-mail, spreadsheets, word-processing documents) and kinds of electronic devices (e.g., network backup tapes, local hard drives and other databases) from which potential sources of electronic discovery can be obtained [see generally *Zubulake v. UBS Warburg LLC* (SDNY 2003) 217 FRD 309, 311 ("[a]s individuals and corporations increasingly do business electronically--using computers to create and store documents, make deals, and exchange e-mails--the universe of discoverable material has expanded exponentially" (footnotes omitted))].

Not only can discoverable information come from paper documents, but also (and more often) from e-mails, word-processing documents, spreadsheets, and PowerPoint presentations. These types of documents can reside on hard drives, CDs, disks, network servers, and backup tapes and other databases [see *Zubulake v. UBS Warburg LLC* (SDNY 2003) 217 FRD 309, 313-315 (discussing various sources of electronically stored e-mail sought by plaintiff in gender discrimination/retaliatory discharge case)]. It is also helpful to know when obtaining a forensic expert to analyze electronic data or an electronic device is necessary].

Counsel should also consider demanding ESI that is of a more esoteric nature or that may be stored in locations other than on a standard computer. Cell phones, personal digital assistants (PDAs), fax machines, answering machines, copiers, printers, digital cameras, and surveillance cameras, among other things, all contain ESI. In addition, the internet itself has become an important source of information that is stored in website descriptions and advertisements, images, blogs, tweets, and social networking sites. All of these sources are subject to the California procedures governing e-discovery and should be considered in formulating the scope of the demand.

Warning:

Attorneys who are largely unfamiliar with e-discovery may think of e-discovery as confined to e-mail, memoranda, spreadsheets and other information stored on computers. In fact, the spectrum of potentially important information subject to the e-discovery rules is much broader than that. Since the statutory definition of ESI is so broad, counsel needs to think equally broadly in considering what ESI should be

the subject of the demand.

6.06[2] Demanding Party Should Consider What Production Format to Specify In Demand. In formulating a demand for production of electronic evidence, counsel should consider what form of the information would be most useful for purposes of the litigation [see *CCP* § 2031.030(a)(2) (demand may specify form in which information is to be produced)]. Some common forms of production of electronically stored information include the following:

- **Native File Format.** The form in which electronically stored information is ordinarily maintained on the computers or other locations of the responding party [see *CCP* § 2031.280(d)(1)] is sometimes called "native format." Native format may include metadata, or hidden information about a particular document, including its date of creation, author, revisions, and file history. Production of electronically stored information in native format may be less expensive. Also, native format typically is searchable, so that key terms can be found easily.

- **Images in PDF and TIFF with a Load File.** PDF (Portable Document Format) and TIFF (Tagged Image File Format) files are digital snapshots of electronic documents. These forms replicate a document's image, but they may not include the accompanying metadata. PDF files may include a searchable text layer that may either be created with the file (e.g., when printing from Microsoft Word to a PDF), or added later using optical character recognition. TIFF files are not searchable, but they may be produced with an associated database load file for litigation support software; this load file may contain searchable text that has either been extracted from the native version of the document (e.g., from an e-mail file), or that has been added by optical character recognition OCR software.

- **Paper.** A party may specify hard copy as the demanded form.

- **Database Queries/Reports Versus Raw Data From a Database.** In seeking ESI from a database, counsel should understand and distinguish between whether the raw data is needed, or whether reports created from the raw data are needed.

A database is a collection of mutually related data or information stored in computer record fields. Databases may track key business information that may be useful in discovery, such as employee information, job classifications, records of sales, and other relevant data. The information in databases is often structured and customized in ways particular to an organization.

Example:

For example, a business database might track sales in one table, customer names in a second table, and customer addresses in a third table. The tables of raw data from the database will be useful only if the data structure and information storage protocols are completely understood so that the receiving party (or its expert) may load the raw data into a database and run its own queries. This raw data from the database will usually be transferred by text load files that indicate the start and end of fields and records.

Alternatively or in addition, the receiving party may seek a report of the underlying data in response to a database query. Thus, if the information sought in the dispute is the names and addresses of customers in California who bought an item in July 2009, a report generated from a query done by the producing party may be more useful than the underlying raw data.

Distinguish--"Native Format" and "Reasonably Usable Form":

If a production demand does not specify a form for production of electronically stored information, the responding party must produce it in native format or in a reasonably usable form [*CCP* § 2031.280(d)(1)]. The term "reasonably usable form" has been interpreted to mean a format that is both

electronically searchable and sortable [*L.H. v. Schwarzenegger* (ED Cal 2008) 2008 US Dist LEXIS 86829, at *12-*13 (construing "reasonably usable form" as used in *Fed R Civ P* 34(a)(1)(A))]. If necessary, the responding party must translate any data compilations included in the demand into a reasonably usable form--at the reasonable expense of the demanding party [CCP § 2031.280(e); see *Toshiba Am. Elec. Components, Inc. v. Superior Court* (2004) 124 CA4th 762, 769-772, 21 CR3d 532 (federal law does not provide for similar cost-shifting)].

**Cross Reference:**

Discussion of electronically stored information terminology, see Ch. 1, Appendix A, Glossary of Technical Terms Encountered in E-Discovery.



59 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 6 Demanding Production of Electronically Stored Information in California Court

II. DETERMINING WHAT TO ASK FOR

1-6 MB Practice Guide: CA E-Discovery and Evidence 6.07

6.07 Party May Demand Copy of Electronic Information.

6.07[1] Copy of Information Is Usually Sufficient to Meet Litigation Needs. A party may demand a copy of electronically stored information that is in the possession, custody, or control of the opposing party [*CCP* § 2031.010(a)]. Demands for "copies" of electronically stored information, rather than demands to inspect or sample originals, are the most common production demand.

Decision Point:

It may be important that the copying (sometimes called data "collection") be done in a way that replicates the data exactly as is and does not change any of its profile characteristics such as metadata (author, recipient, create date, modified date, document type). If so, the production demand should specify that the copy should include such characteristics of the original [*see CCP* § 2031.030(c)(1), (4) (demand may specifically describe each item sought and may specify related activities that are demanded)]. If the electronic information's native format is usable by the demanding party, the demand should specify that format for the demanded copy so as to retain the profile characteristics of the original.

Example:

Copies of e-mail are often demanded and may reside in media such as e-mail exchange servers, hard disk files, or PDAs. A demand for production of copies of e-mail should specify that the production be in a form that preserves searchability, important fielded metadata (e.g., from/to/cc/subject/date) and any files sent as e-mail attachments.



Cross Reference:

Sample production demand, see 6.20.

6.07[2] Demanding Party Should Consider Whether Data Is Reasonably Accessible.

6.07[2][a] Responding Party May Object or Seek Protective Order. If the demand seeks a copy of data that is not reasonably accessible (e.g., from sources that are not routinely accessed or easily located), the responding party may either object [*CCP* § 2031.210(d)] or move for a protective order [*CCP* § 2031.060(a), (b)].

Examples:

Accessibility turns largely on the expense of production. Backup tapes are often considered inaccessible, particularly when they are not organized for retrieval of individual documents or files. Other data sources that might not be reasonably accessible can include legacy data, deleted data, databases that cannot readily create different forms of information than those that they were designed to create, and large volumes of data, such as source code versions [see *OpenTV v. Liberate Techs.* (ND Cal 2003) 219 FRD 474, 476-479] .



Strategic Point:

For either a protective order or a motion to compel, the party claiming that ESI is not reasonably accessible bears the burden of demonstrating that the information is from a source that is not reasonably accessible because of undue burden or expense [CCP §§ 2031.060(c), 2031.310(d)].



Cross Reference:

Discussion of protective orders, see Ch. 11, *Seeking or Opposing Protective Order*, 11.03-11.07.

Discussion of motions to compel, see Ch. 12, *Obtaining or Opposing Motion to Compel*.

6.07[2][b] Court May for Good Cause Order Discovery. In ruling on a motion for a protective order or a motion to compel, the court may order discovery of electronically stored information from a source that is not reasonably accessible if the demanding party shows "good cause" for discovery [CCP §§ 2031.060(d), 2031.310(e)].

The Electronic Discovery Act is silent on what constitutes "good cause" for ordering discovery of information that is not reasonably accessible. However, a California state court might look at the weighing of burdens and costs considered by courts applying federal law, including consideration of the following factors [see Committee Note of 2006 to *Fed R Civ P* 26(b)(2)]:

- 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.
- The parties' resources.

6.07[2][c] Court May Allocate Discovery Expenses. If the court finds good cause for the production of electronic information that is not reasonably accessible, the court may set conditions for discovery, including allocation of the expense of discovery [CCP § 2031.060(e)]. In deciding whether to order cost-shifting, federal courts consider factors such as the following [*OpenTV v. Liberate Techs.* (ND Cal 2003) 219 FRD 474, 476] :

- The extent to which the demand is specifically tailored to discover relevant information.

- The availability of such information from other sources.
- The total cost of production, compared with the amount in controversy.
- The total cost of production, compared with 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.
- The relative benefits to the parties of obtaining the information.

Example:

The responding party argued that by agreeing to make its complete database available for inspection and copying, it had satisfied its obligations by making the source code available for inspection in the order and manner in which it was kept in the ordinary course of business. The court found that it would take between 125 and 150 hours of work to complete the extraction process for the multiple versions of source code sought by the demanding party and that the demanded electronic data was stored in a format that was not reasonably accessible. Since the demanded source code was highly likely to contain relevant information and was unavailable from another source, the court found cost-shifting appropriate. Because the parties were similarly situated (both were corporations), the court ordered the parties to split equally the cost of extracting the source code, with the responding party to bear the cost of making the demanded copy [*OpenTV v. Liberate Techs. (ND Cal 2003) 219 FRD 474, 476-479*] .

**Cross Reference:**

Discussion of demand for inspection, see 6.08[2].



60 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 6 Demanding Production of Electronically Stored Information in California Court

II. DETERMINING WHAT TO ASK FOR

1-6 MB Practice Guide: CA E-Discovery and Evidence 6.08

6.08 Party May Demand to Test, Sample, or Inspect Electronic Information.

6.08[1] Testing or Sampling Allows Determination of Whether Information Is Relevant. A party may demand to test or sample electronically stored information in the possession, custody, or control of the responding party [*CCP* § 2031.010(e)]. Testing or sampling of electronically stored information may be a low-cost option to determine whether a given source contains relevant information.

Consider:

Testing and sampling of a responding party's electronic information system may raise issues of privilege, confidentiality, or privacy. The rule is not meant to create a routine right of direct access to a party's electronic information system.

Distinguish--Demand That Responding Party Perform Testing or Sampling:

The relevant provision of the Civil Discovery Act refers to a demand for testing or sampling by "the party making the demand, or someone acting on that party's behalf" [*CCP* § 2031.010(e)]. This language does not expressly authorize a party to demand sampling by the producing party, but that result (sampling by the producing party) is something that can likely be obtained by meet and confer or a court order [*see, e.g., Toshiba America Electronics Components v. Superior Court* (2004) 124 CA4th 762 (encouraging parties to meet and confer regarding translating a sample of backup tapes); *Zubulake v. UBS Warburg LLC* (SDNY 2003) 217 FRD 309, 324 ("[r]equiring the responding party to restore and produce responsive documents from a small sample of the demanded backup tapes is a sensible approach in most cases")].

6.08[2] Demanding Party May Seek to Inspect Responding Party's Computer System. Rather than simply demanding a copy of ESI, a party may demand to inspect and copy ESI from physical devices storing the electronically stored information [*CCP* § 2031.010(e)]. However, because computer disks often include irrelevant, privileged, and confidential information, courts ordinarily will not allow physical inspection and copying of computer disks unless a showing of improper deletion or spoliation of files has been made [*see, e.g., Dodge, Warren & Peters Ins. Servs., Inc. v. Riley* (2003) 105 CA4th 1414, 1417-1418, 130 CR2d 385 ; *Hedenburg v. Aramark Am. Food Servs. (W.D. Wash. 2007)* 2007 U.S. Dist. LEXIS 3443 (denying "mirror image" request in light of statements by producing party that search was complete; analogizing an inspection order to a search warrant, and noting that the court would not allow an analogous search of plaintiff's property for a lost paper diary)].

Drawback:

Demands for inspection are subject to motions for protective orders and/or objection if the demands are unreasonably cumulative or duplicative, or unduly burdensome or expensive [CCP §§ 2019.030, 2031.060(a)]. The party making an objection or seeking a protective order bears the burden of demonstrating undue burden or expense [CCP § 2031.060(b)].

**Cross Reference:**

Protective orders, see *Ch. 11, Seeking or Opposing Protective Order, 11.03-11.07*.

**Strategic Point--Recoverability of Deleted Files:**

Physical inspection and forensic copying is often used when "deleted" information is sought. Counsel should not assume that deleted computer files are lost forever. Although a file or document on a computer can be deleted or erased by means of the delete function, such information may continue to exist in electronic form on the computer's hard drive until overwritten with new data. Thus, electronic information that has been deleted has not necessarily been destroyed and might, under some circumstances, still be recovered in an inspection of the hard drive [see, e.g., *Antioch Co. v. Scrapbook Borders, Inc. (D Minn 2002) 210 FRD 645, 651-654* (granting motion to appoint expert to attempt to resurrect data that had been deleted from defendants' computer equipment); *Playboy Enters. v. Welles (SD Cal 1999) 60 F Supp2d 1050, 1052-1055* (in trademark suit, e-mails were missing and had been deleted; plaintiff asked for mirror image of computer to retrieve); *Gates Rubber Co. v. Bando Chem. Indus. (D Colo 1996) 167 FRD 90, 112-113* (discussing procedures for recovery of fragments of deleted files)].

**Cross Reference:**

Recovery of deleted files, see *Ch. 1, Understanding Electronic Evidence, 1.22[6], 1.38, 1.40[2]*.

**Strategic Point--Use of Experts:**

An inspection of a party's computer system typically involves having an expert create a forensic copy of the data from a computer disk drive. This copy is sometimes referred to (inaccurately) as a "mirror image." Data from the forensic copy can be later searched for electronically stored information, such as deleted or altered files, unauthorized copies of software, or for other reasons [see CCP § 2031.010(d); see, e.g., *Dodge, Warren & Peters Ins. Servs., Inc. v. Riley (2003) 105 CA4th 1414, 1417-1418, 130 CR2d 385*; *Playboy Enters. v. Welles (SD Cal 1999) 60 F Supp2d 1050, 1054-1055*]. Pursuant to its authority to issue an injunctive order for the preservation of electronically stored information pending discovery, the court may appoint a neutral expert, or require the parties to appoint an expert, to carry out the process of copying, recovering, and storing the relevant information [see *Dodge, Warren & Peters Ins. Servs., Inc. v. Riley (2003) 105 CA4th 1414, 1417, 130 CR2d 385*]. The appointment of a neutral person, such as a special master or forensic expert, also provides protection for potentially privileged information that might be recovered from hard disk inspections. Inspection orders typically provide a mechanism for the producing party to review any data found, and assert privilege or confidentiality as to particular files as appropriate [*Antioch Co. v. Scrapbook Borders, Inc. (D Minn 2002), 210 FRD 645, 652-654* (granting motion to appoint neutral expert in computer forensics); *Simon Prop. Group L.P. v. MySimon, Inc. (SD Ind 2000) 194 FRD 639, 641-642* (use of special master was appropriate to review hard drive for relevant data); *Dodge, Warren & Peters Ins. Servs., Inc. v. Riley (2003) 105 CA4th 1414, 1417, 130 CR2d 385* (affirming order that allowed inspection by court-appointed expert); *Playboy Enters. v. Welles (SD Cal 1999) 60 F Supp2d 1050, 1055* (use of special master was appropriate to

review hard drive for relevant data)].

Cross Reference:

Discussion of selection of e-discovery experts, see *Ch. 4, Planning E-Discovery, 4.11-4.14*. Discussion of procedures, including use of experts, to preserve electronic evidence pending discovery, see *Ch. 7, Obtaining Injunction to Protect Against, Destruction of Electronic Evidence Pending Discovery, 7.03-7.08*.

If the responding party refuses to provide access to its computer system on the ground of undue burden or expense, the demanding party must convince the court that there is good cause for discovery [see *CCP § 2031.060(d)*]. In such a case, the court is more likely to allow inspection of the responding party's computer if (1) there are measures to prevent the disclosure of privileged or other non-discoverable information, such as the appointment of a neutral expert [see *Playboy Enters. v. Welles (SD Cal 1999) 60 F Supp2d 1050, 1055*]; (2) the contents of the computer files are central to a party's claim or defense [see *Hedenburg v. Aramark Am. Food Servs. (WD Wash 2007) 2007 US Dist LEXIS 3443, at *4*]; and (3) ordinary discovery procedures controlled by the responding party are shown to be inadequate, due to factors such as evidence of attempted spoliation of evidence [*Dodge, Warren & Peters Ins. Servs., Inc. v. Riley (2003) 105 CA4th 1414, 1417, 130 CR2d 385*].



Strategic Point:

The court is more likely to issue an order for inspection if the demand is carefully limited in scope and the court is provided with an expert's declaration specifying the method by which the inspection will be conducted [but see *Hedenburg v. Aramark Am. Food Servs. (WD Wash 2007) 2007 US Dist LEXIS 3443, at *4* ("mirror imaging" of a computer hard drive was not allowed where the contents of the computer files were not central to the case and demand was but was an attempt by the defendant to merely impeach the plaintiff)]. Counsel should establish that an inspection of the responding party's computer will locate responsive information, that any inconvenience to the responding party will be justified, and that the chances of harm to the responding party will be minimized [see *Playboy Enters. v. Welles (SD Cal 1999) 60 F Supp2d 1050, 1054-1055*].

Example:

The court granted defendants' motion to compel inspection of a third-party plaintiff's computer when (1) there was a high "level of contention and distrust that permeate[d] the litigation; (2) the third-party plaintiff had adamantly refused to permit "even a limited inspection of the computer"; and (3) there was evidence that another individual plaintiff's computer had been "forensically cleaned" prior to defendants' inspection. The magistrate judge noted that inspection intended to reveal the computer's metadata "is particularly important here, as it will likely include information that may demonstrate whether there has been any transfer or deletion of information, or other efforts to minimize, hinder or prevent access to information ... " [*Dawe et al. v. Corrections USA et al. (ED Cal 2009) 263 FRD 613, 619*].



61 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 6 Demanding Production of Electronically Stored Information in California Court

III. PREPARING AND MAKING DEMAND

1-6 MB Practice Guide: CA E-Discovery and Evidence 6.09

6.09 CHECKLIST: Preparing and Making Demand.

☐ Draft set of demands.

Discussion:

See 6.11

Forms:

See 6.20, 6.21

☐ In first paragraph below title of case, identify following:

Authority:

CCP § 2031.030(b)

☐ Demanding party.

☐ Set number.

☐ Responding party.

☐ Set forth each demand separately, and identify it by number or letter.

Authority:

CCP § 2031.030(c)

☐ Include following in each demand:

☐ Designation of electronically stored information to be inspected, copied, tested, or sampled, either by specifically describing each individual item or by reasonably particularizing each category of item.

Authority:

CCP § 2031.030(c)(1)

☐ Specification of reasonable place and time, not less than 30 days after service of demand, for production of demanded information.

Authority:

CCP § 2031.030(c)(2), (3)

☐ Specification of any inspection, copying, testing, sampling, or related activity that is being demanded, manner in which it will be performed, and whether it will permanently alter or destroy item involved.

Authority:

CCP § 2031.030(c)(4)

☐ If desired, specification of form in which demanded information is to be produced.

Authority:

CCP § 2031.030(a)(2)

☐ Serve set of demands.

Authority:

CCP §§ 2031.020, 2031.040, 2031.290

Discussion:

See 6.12

☐ Serve copy of set of demands on responding party.

☐ Serve copy of set of demands on every other party that has appeared in action.

☐ Do not file set of demands with court, but retain original set and proof of service until six months after final disposition of action.

☐ Review responding party's responses to demands, as well as information produced by responding party.

Authority:

CCP §§ 2031.060, 2031.260, 2031.280

Discussion:

See 6.13

- ☐ If responding party failed to respond timely, move to compel response.

Authority:

CCP § 2031.300

- ☐ If necessary, oppose responding party's motion for protective order.

Authority:

CCP § 2031.060

- ☐ If responding party's response is inadequate, consider whether to move for further response.

Authority:

CCP § 2031.310

- ☐ If responding party's production of information is inadequate, consider whether to move for order compelling compliance.

Authority:

CCP § 2031.320

- ☐ If responding party inadvertently produces some information that is subject to claim of privilege or of protection as attorney work product, promptly return that information.

Authority:

CCP § 2031.285



62 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 6 Demanding Production of Electronically Stored Information in California Court

III. PREPARING AND MAKING DEMAND

1-6 MB Practice Guide: CA E-Discovery and Evidence 6.10

6.10 Options and Strategies.

Counsel must prepare and serve the demand for production, copying, testing, or sampling of ESI in accordance with statutory and regulatory requirements. The demand should describe the information sought and the form in which it is being requested [*see CCP § 2031.030*].

In addition to a demand for production or inspection of electronically stored information, a party may propound a supplemental demand to discover any later acquired electronically stored information [*CCP § 2031.050(a)*]. A party may propound a supplemental demand twice before the initial setting of the trial date, and once after the initial setting of the trial date [*CCP § 2031.050(b)*]. In addition, on motion and for good cause, the court may grant a party leave to propound additional supplemental demands [*CCP § 2031.050(c)*].



63 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 6 Demanding Production of Electronically Stored Information in California Court

III. PREPARING AND MAKING DEMAND

1-6 MB Practice Guide: CA E-Discovery and Evidence 6.11

6.11 Production Demand Must Comply With Formal Requirements.

6.11[1] Demand Must Meet Prescribed Format and Content Requirements.

6.11[1][a] Demands Must Be Consecutively Numbered. Each set of production demands must be numbered consecutively [*CCP* § 2031.030(a)(1)].

6.11[1][b] First Paragraph Must Contain Identifying Information. The first paragraph immediately below the title of the case must identify all of the following [*CCP* § 2031.030(b)]:

- The demanding party.
- The set number.
- The responding party.

6.11[1][c] Each Demand Must Be Separately Identified. Each demand in the set must be separately set forth and be identified by number or letter [*CCP* § 2031.030(c)].

6.11[1][d] Each Demand Must Specify Item or Category of Item Being Demanded. Each demand must designate the electronically stored information to be inspected, copied, tested, or sampled, either by specifically describing each individual item or by reasonably particularizing each category of item [*CCP* § 2031.030(c)(1)].

Drawback--Restricted Discovery in Limited Civil Case:

In a limited civil case (typically, a case in which the amount or value of property in controversy does not exceed \$25,000 [*see CCP* §§ 85, 86, 86.1]), the number of discovery demands is restricted. With the exception of small claims or unlawful detainer cases, a party in a limited civil case is limited to a combination of 35 of the following forms of discovery: interrogatories, production demands, and demands for admission [*CCP* §§ 91, 94(a); *see CCP* §§ 2030.010, 2031.010, 2033.010].

6.11[1][e] Demand Must Specify Time for Inspection. Each demand must specify a reasonable time for the inspection, copying, testing, or sampling that is at least 30 days after service of the demand, unless the court for good cause shown has granted leave to specify an earlier date [*CCP* § 2031.030(c)(2)].

Exception:

In an unlawful detainer action or similar proceeding [*see CCP § 1159 et seq.*], the demand must specify a reasonable time for the inspection, copying, testing, or sampling that is at least five days after service of the demand, unless the court, for good cause shown, has granted leave to specify an earlier date [*CCP § 2031.030(c)(2)*].

6.11[1][f] Demand Must Specify Place for Inspection. The demand must specify a reasonable place for making the inspection, copying, testing, or sampling, and for performing any related activity [*CCP § 2031.030(c)(3)*].

6.11[1][g] Demand Must Specify Type and Manner of Activity Being Demanded. The demand must specify any inspection, copying, testing, sampling, or related activity that is being demanded, as well as the manner in which that activity will be performed, and whether that activity will permanently alter or destroy the item involved [*CCP § 2031.030(c)(4)*].

**Trap:**

The propounding party should consider the cost of any related activity to be conducted. The demanding party cannot compel the responding party to share the cost [*see San Diego Unified Port Dist. v. Douglas E. Barnhart, Inc. (2002) 95 CA4th 1400, 1405, 116 CR2d 65* (defendants could not be required to share in the cost of destructive testing they did not want)].

6.11[1][h] Demand Should Specify Form of Production. The demand may specify the form or forms in which each type of electronically stored information is to be produced [*CCP § 2031.030(a)(2)*]. The demanding party may ask for different forms of production for different types of electronically stored information. However, the demand may not require more than one form of production for the same electronically stored information [*see CCP § 2031.280(d)(2)*].

**Warning:**

If a production demand does not specify a form for production of electronically stored information, the responding party must produce it in native format or in a reasonably usable form [*CCP § 2031.280(d)(1)*]. Therefore, unless counsel is certain that the information's native format (or the responding party's concept of a reasonably usable form) will be acceptable, the better practice is to specify in the demand a form for production of the information. If the demand specifies a form other than native format, the demanding party may be required to pay the cost of translating any data compilations included in the demand into the required format [*CCP § 2031.280(e)*].

Example--Failure to Specify Form of Production in Initial Document Request:

Plaintiffs did not specify the form of production or ask for metadata in their initial document request. After defendant had gathered and produced nearly the entire production of Word documents, Excel spreadsheets, and approximately 500 e-mails in text-searchable PDF format, and produced search results from three separate databases in paper format, plaintiff demanded metadata. Plaintiff asked the court to compel defendant to produce e-mails and electronic documents in TIFF format with a corresponding load file containing metadata fields and extracted text, and produce the spreadsheets and databases in native format. The court ruled that plaintiff would have to pay defendant's costs of producing Word and PowerPoint files a second time if plaintiff wanted the metadata, and that defendant only had to produce metadata for 200 e-mails that had been collected in a manner that preserved the metadata. The court denied the plaintiff's request for metadata from one of the databases and ordered the parties to conduct a live demonstration of the operation of the other two databases to allay plaintiff's lawyers' concern that they would not know if they had received all of the responsive information from the database without access to the metadata [*Aguilar v. Immigration and Customs Enforcement Division of the U.S. Dept. of Homeland Security (SDNY 2008) 225 FRD 350*].

Cross Reference:

Discussion of native format and reasonably usable form, see 6.06.

Consider:

The demanding party should consider the following in selecting a form for production: (1) whether it will be useful or necessary that the produced data be searchable, (2) whether the metadata is needed, and (3) whether selecting a particular form will affect the cost of discovery. Different forms of production may be appropriate for different types of data. For example, e-mails and word processing documents usually print well, and a party may demand production of these files as TIFF or PDF images with associated litigation database load files to maintain their searchability and sortability. In contrast, Excel spreadsheets often do not print well when converted to TIFF or PDF and the formulas contained in the calculating cells may be lost, so production of these files in native Excel format may be preferable.

Cross Reference:

Discussion of forms of electronically stored information, see Ch 1, Understanding Electronic Evidence.

6.11[2] Demand Should Be Tailored to Specific Facts of Case. A demand for the production of electronically stored information should be tailored to the specific facts and circumstances of the case, so as to avoid objections by the responding party [CCP § 2031.030(c)(1)].

In drafting the demand, the demanding party should support the factual components of a cause of action, theory of liability, or defense with enough information to support each element identified [see *generally* Principle 4, The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production (2004), available at [http://www.thosedonaconference.org/dltForm?did=Sedona Principles200401.pdf](http://www.thosedonaconference.org/dltForm?did=Sedona%20Principles200401.pdf) ("[d]iscovery requests should make as clear as possible what electronic documents and data are being asked for, while responses and objections to discovery should disclose the scope and limits of what is being produced")].

6.11[3] Demand Should Not Be Overbroad or Unduly Burdensome. Demands for production of electronically stored information should not be overbroad or unduly burdensome. In determining whether discovery of electronically stored information will be unduly burdensome to the responding party, the court weighs the benefit and burden of the discovery. In so doing, the court considers the circumstances of the case, the amount in controversy, the particular issues at stake, and the potential for finding relevant material [*Playboy Enters. v. Welles* (SD Cal 1999) 60 F Supp2d 1050, 1054] .

Strategic Points:



- The broader the scope of production of electronically stored information, the more difficult and burdensome it may be for the responding party to identify, preserve, and review the electronically stored information. Moreover, an overbroad demand may invite a "data dump" that leaves the demanding party with the burden of culling out the relevant information [see *Jackson v. City of San Antonio* (WD Tex 2006) 2006 US Dist LEIS 8091, at *4 (production was not impermissible "data dump" because it was responsive to demand, and burden of culling out relevant information was substantially same for both sides)].

- The demanding party should seek only the documents it really needs, based on the facts of the case and the results obtained from other discovery demands and interrogatories. Counsel should make sure, though, that the demand is not so narrow that it misses the opportunity to obtain some relevant data.

Example:

In a federal suit alleging age discrimination and fraud, the plaintiff sought discovery of a "computer diskette or tape copy of all word processing files created, modified and/or accessed by, or on behalf" of five employees of the defendant over a two-and-a-half-year period. The court of appeals affirmed the trial court's denial of the plaintiff's motion to compel production. The appellate court noted that the plaintiff "has not tried to identify particular items within the expansive request nor has he provided a theory of relevance that might narrow the scope of his request" [*Wright v. AmSouth Bancorporation* (11th Cir 2003) 320 F3d 1198, 1205] .



64 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 6 Demanding Production of Electronically Stored Information in California Court

III. PREPARING AND MAKING DEMAND

1-6 MB Practice Guide: CA E-Discovery and Evidence 6.12

6.12 Propounding Party Must Serve Demand.

6.12[1] Demand May Be Served Within Times Authorized by Statute. A defendant may serve a demand for the production of electronically stored information without leave of court at any time [CCP §§ 2031.020(a), 2031.040].



Timing:

A plaintiff may serve a demand for the production of electronically stored information without leave of court at any time that is 10 days or more after the earlier of service of the summons on, or appearance by, the party to whom the demand is directed [CCP §§ 2031.020(b), 2031.040].

Exceptions:

In an unlawful detainer action or similar proceeding [see CCP § 1159 *et seq.*], a plaintiff's demand for production may be served as soon as five days after the earlier of service of the summons on, or appearance by, the party to whom the demand is directed [CCP § 2031.020(c)]. In any case, however, the court, for good cause shown, may shorten the time for serving a demand for production [CCP § 2031.020(d)].

6.12[2] Copy of Demand Must Be Served on All Other Parties. A copy of the production demand must be served not only on the party to whom it is directed, but also on every other party that has appeared in the action [CCP § 2031.040].

6.12[3] Demand Is Not Filed With Court. A demand for production of electronically stored information is not filed with the court [CCP § 2031.290(a); see *Cal Rules Ct*, Rule 3.250(a)(9)].

6.12[4] Demanding Party Must Retain Original Demand and Response. The demanding party must retain both the original of the demand, with the original proof of service affixed, and the original of the responding party's sworn response until six months after final disposition of the action [CCP § 2031.290(b); *Cal Rules Ct*, Rule 3.250(b)]. Six months after final disposition of the action, the original demand may be destroyed, unless the court, on motion of any party and for good cause shown, orders that the originals be preserved for a longer period [CCP § 2031.290(b); *Cal Rules Ct*, Rule 3.250(b)].



65 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 6 Demanding Production of Electronically Stored Information in California Court
III. PREPARING AND MAKING DEMAND

1-6 MB Practice Guide: CA E-Discovery and Evidence 6.13

6.13 Demanding Party Should Review Response and Production.

6.13[1] Responding Party Must Serve Timely Response. The party to whom a demand for production of electronically stored information is directed ordinarily must serve a response to the demand within 30 days after service of the demand [CCP § 2031.260(a)]. The response must be signed under oath unless it contains only objections [CCP § 2031.250]. The original of the response must be served on the demanding party, with copies served on other parties who have appeared in the action [CCP § 2031.260(a)]. If a timely response is not served, the propounding party may move for an order compelling a response [CCP § 2031.300(b)].

Exceptions:

In an unlawful detainer action or similar proceeding [see CCP § 1159 *et seq.*], the usual time to respond is five days after service of the demand [CCP § 2031.260(b)]. In any case, however, the court on motion by the propounding or responding party, may shorten or extend the time for responding to the demand [CCP § 2031.260(a), (b)]. In any case, the parties may agree in writing to an extended date for serving a response [CCP § 2031.270(a), (c)].

➤ Cross References:

Detailed discussion of the required contents of a response to a demand for production of electronically stored information, see *Ch. 8, Responding to Electronic Discovery Demands in California Court*, 8.12-8.23.

Moving to compel response, see *Ch. 12, Obtaining or Opposing Motion to Compel*.

Detailed discussion of respondent's production of ESI, see *Ch. 9, Gathering and Producing Electronically Stored Information*, 9.47-9.56.

Detailed discussion of objections to demands for production of ESI, see *Ch. 10, Opposing Demands for Production of Electronic Evidence in California Court*, 10.09-10.14.

6.13[2] Counsel Should Determine Whether to Move to Compel Further Response or Compliance With Demand. Counsel for the demanding party should promptly review the response, and the electronic information

produced pursuant to the response, to determine whether they satisfy the demand. If not, counsel should consider whether to make a motion to compel a further response or to compel compliance with the demand [*see CCP §§ 2031.310, 2031.320*]. If no timely response is served, counsel should move to compel a response [*see CCP § 2031.300*].

**Timing:**

The demanding party will forfeit the right to compel a further response if notice of a motion to compel is not given within 45 days of the service of the response [*CCP § 2031.310(c)*].

**Cross Reference:**

Making or opposing motion to compel a response or further response, or motion to compel compliance with a demand for production, see Ch. 12, Obtaining or Opposing Motion to Compel.

6.13[3] Demanding Party Must Promptly Return Privileged Information That Was Inadvertently Produced.

If the demanding party receives notice from a party that the electronic information produced includes some information that is subject to a claim of privilege or of protection as attorney work product [*see CCP § 2031.285(a)* (notice must include basis for claim of privilege or work-product protection)], the demanding party must immediately sequester the specified information and either (1) return the information and any copies that may exist, or (2) present the information to the court conditionally under seal for a determination of the privilege or work-product claim [*CCP § 2031.285(b)*]. If the information is presented to the court under seal, the demanding party then has 30 days to make a motion for determination of the claim of privilege or work-product protection [*CCP § 2031.285(d)(1)*]. Until the legitimacy of the claim of privilege or protection is resolved, the demanding party must preserve the information and keep it confidential, and may not use the information in any manner [*CCP § 2031.285(c)(1), (d)(2)*]. If the demanding party disclosed any of the information before receiving notice of the claim of privilege or protection, the demanding party must take reasonable steps to retrieve the information after receiving notice of the claim [*CCP § 2031.285(c)(2)*].

**Cross Reference:**

Handling of inadvertently disclosed information that is privileged or protected as work product, see Ch. 3, *Ethical Issues for Attorneys in E-Discovery*, 3.14, 3.15.



66 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 6 Demanding Production of Electronically Stored Information in California Court

IV. OBTAINING ELECTRONIC INFORMATION FROM NONPARTY

1-6 MB Practice Guide: CA E-Discovery and Evidence 6.14

6.14 CHECKLIST: Obtaining Electronic Evidence From Nonparty.

- ☐ Ascertain that electronically stored information sought cannot be obtained from any party to action.

Authority:

Calcor Space Facility, Inc. v. Superior Court (1997) 53 CA4th 216, 225, 61 CR2d 567

Discussion:

See 6.16

- ☐ Ascertain whether ESI in question is likely to be in possession of a third party.

Authority:

CCP § 1985.8

Discussion:

See 6.16

- ☐ Prepare subpoena commanding nonparty to produce electronically stored information.

Authority:

CCP § 1985.8

Discussion:

See 6.17

Form:

See 6.22

- ☐ Designate electronically stored information to be inspected, copied, tested, or

sampled, either by specifically describing each item or by reasonably particularizing each category of item.

Authority:

CCP §§ 1985.8(a),(j), 2020.410(a), 2031.030(c)(1); Calcor Space Facility, Inc. v. Superior Court (1997) 53 CA4th 216, 222, 61 CR2d 567

- ☐ Specify reasonable time and place for production of demanded information, taking care not to impose undue burden or expense on subpoenaed person.

Authority:

CCP § 1985.8(j)

Discussion:

See 6.18

- ☐ If desired, specify form in which demanded information is to be produced.

Authority:

CCP § 1985.8(b)

- ☐ Have subpoena served on person to whom it is directed.

Authority:

CCP § 1985.8

Discussion:

See 6.18

- ☐ Review response to subpoena.

- ☐ If subpoenaed person opposes subpoena because of undue burden or expense, demonstrate to court that good cause exists for discovery.

Authority:

CCP § 1985.8(d)-(f)

Discussion:

See 6.19[1]

- ☐ If appropriate, seek sanctions for noncompliance with subpoena.

Authority:

CCP §§ 1985.8(k)(1), 1992, 2020.240

Discussion:

See 6.19[3]

- ☐ If responding party inadvertently produces some information that is subject to claim of privilege or

of protection as attorney work product, promptly return that information.

Authority:

CCP §§ 1985.8(i), 2031.285



67 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 6 Demanding Production of Electronically Stored Information in California Court
IV. OBTAINING ELECTRONIC INFORMATION FROM NONPARTY

1-6 MB Practice Guide: CA E-Discovery and Evidence 6.15

6.15 Options and Strategies.

Before pursuing discovery from a nonparty, counsel should attempt to obtain the desired electronically stored information from a party to the action. The costs and burdens of discovery ordinarily should not be placed on nonparties if a party possesses the information sought. However, discovery may be had from a nonparty despite a party's possession of relevant information, if the information in the parties' possession is unreliable and may be subject to impeachment by information from a nonparty [*Calcor Space Facility, Inc. v. Superior Court* (1997) 53 CA4th 216, 225, 61 CR2d 567] .



Cross Reference:

Availability of discovery from nonparty, see 6.16.



68 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 6 Demanding Production of Electronically Stored Information in California Court
IV. OBTAINING ELECTRONIC INFORMATION FROM NONPARTY

1-6 MB Practice Guide: CA E-Discovery and Evidence 6.16

6.16 Party May Subpoena Electronically Stored Information From Nonparty.

6.16[1] Discovery From Nonparty Is Available If Party Does Not Possess Reliable Evidence. A party may obtain production of relevant electronically stored information from a person who is not a party to the action. Discovery from a nonparty generally is available only if a party does not possess the material sought to be discovered, or if the material possessed by a party is unreliable and may be subject to impeachment by information from a nonparty [*Calcor Space Facility, Inc. v. Superior Court* (1997) 53 CA4th 216, 225, 61 CR2d 567 (cost and burdens of discovery should be placed on nonparties only if parties do not possess information sought or information in their possession is unreliable and may be subject to impeachment by information nonparty possesses)].



Strategic Point:

Electronically stored information possessed by a person who is not a named party to the action, but who is subject to the control of a named party (such as an employee of a named party), may be obtained by discovery directed to that party. Generally, a party can be required to produce not only the electronically stored information that the party possesses, but also information that is in the party's "control" [CCP § 2031.010(d)].

6.16[2] Subpoena May Require Production of ESI. A subpoena in a civil proceeding may require that electronically stored information be produced and that the party serving the subpoena, or someone acting on the party's demand, be permitted to inspect, copy, test, or sample the information [CCP § 1985.8(a)(1)]. Although a subpoena may seek a deposition of the person producing the records, often all that will be required of the subpoenaed person is the production of the ESI, along with an affidavit authenticating the information [see CCP § 2020(a); Evid Code § 1561, CCP §§ 1985, 2020.210 et seq.].



69 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 6 Demanding Production of Electronically Stored Information in California Court
IV. OBTAINING ELECTRONIC INFORMATION FROM NONPARTY

1-6 MB Practice Guide: CA E-Discovery and Evidence 6.17

6.17 Subpoena for Electronically Stored Information Must Comply With Statutory Requirements.

6.17[1] General and Special Subpoena Requirements Apply to Subpoena for ESI.

6.17[1][a] General Subpoena Rules Apply to ESI. Any subpoena requiring the production of electronically stored information must comply with all of the requirements and procedures for the issuance and service of subpoenas generally [*CCP* § 1985.8(a)(2); *see CCP* § 1985 *et seq.*]. Those requirements include special procedures that must be followed when consumers' personal records or employees' employment records are sought [*see CCP* §§ 1985.3, 1985.6, 2020.510(c), (d)].

Cross Reference:

Coverage of general requirements and procedures for issuance and service of subpoena, *see Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 6, 6.12-6.21.*

6.17[1][b] Special Subpoena Requirements Apply to ESI. In addition to the general subpoena requirements, the subpoena must comply with specific requirements that apply to a subpoena for electronically stored information [*see CCP* § 1985.8].

Cross Reference:

Discussion of special requirements applicable to subpoena for electronically stored information, *see 6.17[3], [4], 6.18, 6.19.*

Distinguish:

Special procedures apply to a subpoena that commands only the production of business records for photocopying [*see CCP* § 2020.410 *et seq.*; *see also CCP* §§ 2020.420 (requiring that deposition officer be registered professional photocopier or exempt from registration requirements); 2020.430(a)(1) (requiring production of "true, legible, and durable" copy of subpoenaed business records)]. It appears that those procedures contemplate the production of paper records and are not intended to govern the production of electronically stored information. However, those procedures may provide guidance as to matters not expressly addressed in the statutory provisions specifically governing subpoenas for electronic information.

 Cross Reference:

Coverage of special procedures for subpoena commanding only production of business records for photocopying, see *Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 6, 6.17*.

6.17[2] Subpoena Is Issued by Clerk of Court or by Counsel. The clerk of the court in which the action is pending may issue a subpoena signed and sealed, but otherwise in blank, to a party demanding it; the party then fills it in before service [CCP § 2020.210(a)].

Alternatively, and more commonly, an attorney of record for any party may sign and issue a subpoena, which need not be sealed. A copy may be served on the nonparty, and the attorney may retain the original [CCP § 2020.210(b)].

Similarly, any party to litigation pending outside of California can retain California local counsel who may issue a California subpoena for a nonparty's records (including ESI) located in California [CCP § 2029.350]. Alternatively, a litigant may apply to the clerk of the court to issue the subpoena [CCP § 2029.300].

 Cross Reference:

Discussion of opposing a third-party subpoena, see 6.19[1].

6.17[3] Subpoena Should Designate ESI and Date of Production. The subpoena should designate the electronically stored information to be inspected, copied, tested, or sampled, either by specifically describing each item or by reasonably particularizing each category of item [see CCP §§ 2020.410(a), 2031.030(c)(1); *Calcor Space Facility, Inc. v. Superior Court* (1997) 53 CA4th 216, 222, 61 CR2d 567 (categories must be reasonably particularized from point of view of person who is subjected to burden of producing materials)].

A subpoena for electronically stored information may specify the form or forms in which each type of electronically stored information is to be produced [CCP § 1985.8(b)].

The subpoena should also designate a date for production of the electronically stored information [see CCP § 2031.030(c)(2)].

6.17[4] Subpoenaed Person Must Be Protected From Undue Burden or Expense. A party serving a subpoena requiring the production of electronically stored information must take reasonable steps to avoid imposing undue burden or expense on the subpoenaed person [CCP § 1985.8(j)]. Similarly, any court order requiring compliance with a subpoena for the production of electronically stored information must protect a person who is neither a party nor a party's officer from undue burden or expense resulting from compliance [CCP § 1985.8(k)].

Example:

In an employment discrimination suit, the defendant subpoenaed the plaintiff's e-mail provider, seeking all of the plaintiff's e-mails for a period of six years. The court quashed the subpoena on multiple grounds. The court first held that the federal Stored Communications Act [18 USC §§ 2701-2712] ("SCA") prohibited plaintiff's e-mail provider from disclosing the contents of the e-mails in response to a subpoena in a civil matter. The court also quashed the subpoena on the alternate ground that the subpoena was unduly burdensome. The court remarked that even though some potentially relevant material might be contained in those six years of e-mails, "[t]his is the all too familiar fishing expedition which this court does not countenance" [*Hone v. Presidente U.S.A., Inc.* (ND Cal 2008) 2008 US Dist LEXIS 55722, at *5-*6] .

6.17[5] Federal Stored Communications Act Limits Subpoenas to Electronic Communications Services. The federal Stored Communications Act [18 USC §§ 2701-2712] (SCA) prohibits e-mail service providers from disclosing the contents of e-mails in response to a third-party subpoena in a civil matter [*O'Grady v. Superior Court* (2006) 139

CA4th 1423, 1432, 44 CR3d 72]. Issuing a subpoena to an e-mail service provider for an opponent's e-mails can result in civil liability to the opposing party if the provider violates the SCA by complying with the invalid subpoena [*Theofel v. Farey-Jones* (9th Cir 2003) 341 F3d 978, amended 359 F3d 1066 (9th Cir 2004) (reversing district court's dismissal of suit under SCA against attorney who had obtained plaintiff's e-mails from his Internet service provider by issuing a subpoena)]. The SCA authorizes aggrieved plaintiffs to recover compensatory damages of at least \$1,000, punitive damages, and reasonable attorney's fees and litigation costs in a civil suit [*18 USC § 2707(c)*].

For the same reason, an attorney attempting to subpoena a user's text messages from a cell phone carrier may also run afoul of the SCA. As with an e-mail service provider, a cell phone service provider is an "electronic communication service" under *18 USC § 2510(15)* [see *Jayne v. Sprint PCS* (E.D. Cal. Feb. 19, 2009) 2009 U.S. Dist. LEXIS 13080]. It is therefore a provider of an electronic communication service under the SCA [*11 USC § 2711(1)*].



Strategic Point--Demand Opponent's Consent to Disclosure:

The SCA allows an electronic communication service (ECS) to disclose the contents of e-mails "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service" [*18 USC § 2702(b)(3)*]. Counsel who want to subpoena an opposing party's e-mails from an Internet service provider or text messages from a cell phone provider should first demand the opponent's consent. If the opponent refuses to consent, counsel can move for discovery sanctions [see *O'Grady v. Superior Court* (2006) 139 CA4th 1423, 1446, 44 CR3d 72].

Example:

A judgment of dismissal was affirmed after the claimant refused a discovery order to sign an authorization for the release of medical records [*Miranda v. 21st Century Ins. Co.* (2004) 117 CA4th 913, 929, 12 CR3d 159].



Strategic Point--Request for Identity of Anonymous Poster Does Not Violate SCA.

A litigant seeking to obtain only the *identity* of an anonymous poster on a chat site can do so without running afoul of the SCA if the litigant limits the subpoena to a request for information about the subscriber who posted the message. The plaintiff must make a prima facie showing of the elements of libel in order to overcome a defendant's motion to quash a subpoena seeking the defendant's identity [*Krinsky v. Doe 6* (2008) 159 CA4th 1154, 1164-1165, 72 CR3d 231]. If the plaintiff fails to make a prima facie showing of the elements of libel and the anonymous poster prevails on the motion to quash a subpoena issued in California in connection with an action pending in another state or in a foreign nation, the court must award the anonymous poster his or her costs and reasonable attorney's fees in making the motion to quash [*CCP § 1987.2(b)*].

6.17[6] Federal Stored Communications Act Governs Third-Party Subpoenas to Social Networking Sites. A social networking website is a "person or entity providing remote computing service to the public" under the Federal Stored Communications Act [see *18 U.S.C. § 2702(a)(2)*]. Therefore, attempts to subpoena a social networking site user's non-public content are likely to be met with an objection from the site and refusal to produce the information. The law in this area is developing.

Example:

MySpace takes the position that user content such as private mail messages or stored content files including friend lists, photos, and blogs cannot be produced in response to a third-party subpoena without the user's consent [see *Ledbetter v. Wal-Mart Stores, Inc.* (D. Co. March 27, 2009) Civil Action

No. 06-cv-01958-WYD-MJW, Docket Document #175, Exhibit 8 to Plaintiff's Motion for Protective Order Pursuant to *Fed. R. Civ. P. 26(c)* Regarding Subpoenas Issued to Facebook, My Space, Inc. and Meetup.Com]. In one case, a party issued third-party subpoenas to social networking sites to obtain non-public information posted by two plaintiffs in order to counter plaintiffs' claims they had suffered injuries that prevented them from enjoying their hobbies and outdoor activities. Photos the plaintiffs had posted to the publicly available portions of their pages apparently contradicted their claims that their injuries prevented them from enjoying their outdoor hobbies. In their motion for a protective order, plaintiffs asked the court to order the social networking sites to produce the subpoenaed information directly to the court for in camera review prior to production. The court denied the motion, holding that the existing protective order in the case was sufficient to protect the information [*Ledbetter v. Wal-Mart Stores, Inc.* (D. Co. April 2009) 2009 U.S. Dist. LEXIS 126859]. The court did not discuss the Stored Communications Act. Neither the plaintiffs nor WalMart had briefed the application of the SCA to the third-party subpoenas, despite the fact that MySpace cited the SCA in its original subpoena response in refusing to produce non-public information. Presumably the plaintiff--by asking the court to order production of the documents (albeit for in camera review)--had consented to the release of the information.

Strategic Point:

Although subpoenaing a social networking site member's non-public information directly from the site is likely to draw a refusal to produce the information based upon the Stored Communications Act, a litigant can always issue a discovery request to an opposing party for the information. In *Mackelprang v. Fid. Nat'l Title Agency of Nev., Inc.* (D NV. 2007) 2007 U.S. Dist. LEXIS 2379, 25-26, the defendant issued subpoenas to MySpace to obtain the identity of the holder of several accounts that appeared to be the plaintiff's, and to obtain all of the non-public information posted by the account holder. When MySpace refused to release non-public information posted by the user, the defendant asked the court for an order compelling the plaintiff to sign a consent to the production of all of the private information she may have posted on MySpace. The court held that, assuming the accounts actually belonged to the plaintiff, some non-public information on the MySpace pages could conceivably be relevant to assessing the cause of plaintiff's emotional distress claims, and instructed that "the proper method for obtaining such information, however, is to serve upon [p]laintiff properly limited requests for production" of the relevant information.

Cross References:

Social networking sits as a source of ESI, see 1.32[6].

Discussion of ethical pitfalls in gathering evidence via social networking sites, see 3.09[3].



70 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 6 Demanding Production of Electronically Stored Information in California Court

IV. OBTAINING ELECTRONIC INFORMATION FROM NONPARTY

1-6 MB Practice Guide: CA E-Discovery and Evidence 6.18

6.18 Subpoena Must Be Served.

The subpoena must be served on the subpoenaed person a sufficient time in advance of the designated date of production to provide a reasonable opportunity to locate and produce the designated electronically stored information [CCP § 2020.210(a)].



Timing:

The statutory provisions specifically applicable to subpoenas for electronically stored information do not mandate any minimum time span that the subpoena must allow between service of the subpoena and production of the information sought [see CCP § 1985.8]. The statutory provision governing subpoenas for the production of business records for photocopying requires that such a subpoena command production no earlier than 20 days after issuance of the subpoena, or 15 days after service, whichever is later [see CCP § 2020.410(c)]. The Civil Discovery Act, however, provides a more realistic guideline: a party to whom a demand for production of electronically stored information is directed ordinarily has 30 days to serve a response to the demand [CCP § 2031.260(a)]. Therefore, to avoid a possible claim of undue burden [see CCP § 1985.8(d)], counsel preparing a subpoena for electronically stored information should allow at least 30 days for the nonparty to respond and produce the information sought. As a practical matter, the volume of electronically stored information and the difficulties in gathering and reviewing it for production might require more than 30 days for production. Often, the subpoenaing party and the subpoenaed person agree on a mutually acceptable schedule for production.



Cross Reference:

Discussion of subpoenaing party's duty not to cause undue burden or expense for subpoenaed person, see 6.17[4].

When the subpoena is directed to a natural person, any person may serve the subpoena by personal delivery of a copy of it to the subpoenaed person [CCP § 2020.210(b)(1)]. If the subpoena is directed to an organization, service may be accomplished by delivering a copy of the subpoena to any officer, director, custodian of records, or to any agent or employee authorized by the organization to accept service of a subpoena [CCP § 2020.210(b)(1)].



71 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 6 Demanding Production of Electronically Stored Information in California Court
IV. OBTAINING ELECTRONIC INFORMATION FROM NONPARTY

*1-6 MB Practice Guide: CA E-Discovery and Evidence 6.19***6.19 Subpoenaed Person Must Comply With or Oppose Subpoena.**

6.19[1] Subpoenaed Person May Oppose Subpoena Based on Undue Burden or Expense. If the subpoenaed person opposes the subpoena because the information sought is from a source that is not reasonably accessible because of undue burden or expense, the subpoenaed person bears the burden of demonstrating that those grounds exist [*CCP* § 1985.8(d)].

Even if the information is from a source that is not reasonably accessible because of undue burden or expense, the court may nonetheless order discovery if the subpoenaing party shows good cause [*CCP* § 1985.8(e)]. If the court finds good cause for the production of electronically stored information from a source that is not reasonably accessible, the court may set conditions for the discovery of the electronically stored information, including allocation of the expense of discovery [*CCP* § 1985.8(f)].

A nonparty located in California who receives a third-party subpoena issued in connection with out-of-state litigation pursuant to the Interstate and International Depositions and Discovery Act [*CCP* § 2029.100 *et seq.*] may object to the subpoena on the same grounds as a subpoena issued in connection with California litigation, including the ground that the information is from a source that is not reasonably accessible because of undue burden or expense [*CCP* § 2031.500].

**Strategic Point--Court Imposed Limits:**

Even as to reasonably accessible information, the court must limit the frequency or extent of discovery if the court determines that any of the following conditions exists [*CCP* § 1985.8(h)]:

- It is possible to obtain the information from some other source that is more convenient, less burdensome, or less expensive.
- The discovery sought is unreasonably cumulative or duplicative.
- The party seeking discovery has had ample opportunity by discovery in the action to obtain the

information sought.

- The likely burden or expense of the proposed discovery outweighs the likely benefit, taking into account the amount in controversy, the resources of the parties, the importance of the issues in the litigation, and the importance of the demanded discovery in resolving the issues.

6.19[2] If Subpoenaed Person Does Not Oppose Subpoena, or Opposition Is Overruled, Electronic Information Must Be Produced. If no opposition to the subpoena is pending or sustained, the subpoenaed person must produce the designated electronically stored information [see *CCP* § 2020.220(c)(2)].

Unless the subpoenaing party and the subpoenaed person otherwise agree or the court otherwise orders, if the subpoena does not specify a form for the information, the subpoenaed person must produce the information in the form in which it is ordinarily maintained or a form that is reasonably usable [*CCP* § 1985.8(c)(1)]. In any event, unless otherwise agreed or ordered, the subpoenaed person need not produce the same electronically stored information in more than one form [*CCP* § 1985.8(c)(2)].

If necessary, the subpoenaed person, at the reasonable expense of the subpoenaing party, must, through detection devices, translate any data compilations included in the subpoena into a reasonably usable form [*CCP* § 1985.8(g)].

6.19[3] Subpoenaed Person May Be Sanctioned for Noncompliance. A subpoenaed person is subject to a contempt sanction for failure to comply with a subpoena, even without a prior court order directing compliance [*CCP* § 2020.240]. A \$500 penalty may also be imposed for a failure to appear [*CCP* §§ 1992, *CCP* § 2020.220(c)(2)].

Exception:

In the absence of exceptional circumstances, the court may not impose sanctions on a subpoenaed person or any attorney for a subpoenaed person for failure to provide electronically stored information that has been lost, damaged, altered, or overwritten as the result of the routine, good-faith operation of an electronic information system [*CCP* § 1985.8(k)(1)]. However, this provision does not alter any obligation to preserve discoverable information [*CCP* § 1985.8(k)(2)].

➡ **Cross Reference:**

Detailed discussion of sanctions for failure to obey deposition subpoena, see *Matthew Bender(R) Practice Guide: California Civil Discovery*, Ch. 6, 6.21.

6.19[4] Subpoenaing Party Must Promptly Return Privileged Information That Was Inadvertently Produced. If the subpoenaed person notifies the subpoenaing party that electronically stored information produced pursuant to a subpoena is subject to a claim of privilege or of protection as attorney work product, the subpoenaing party must immediately sequester the specified information and either (1) return the information and any copies that may exist, or (2) present the information to the court conditionally under seal for a determination of the privilege or work-product claim [*CCP* §§ 1985.8(i), 2031.285(b)]. In such a case, the same procedures apply as when a party inadvertently produces privileged or protected material [*CCP* §§ 1985.8(i), 2031.285].

➡ **Cross Reference:**

Discussion of procedures when party inadvertently produces privileged or protected material, see 6.13[3].

Matthew Bender Practice Guide: California E-Discovery and Evidence

Chapter 6 Demanding Production of Electronically Stored Information in California Court
V. FORMS

6.20 Sample Demands for Production of Electronically Stored Information.

COUNTY OF FARALLON

Defendant.

No. _____
PLAINTIFF'S FIRST SET OF
DEMANDS TO DEFENDANT FOR
PRODUCTION OF DOCUMENTS,
INCLUDING ELECTRONICALLY
STORED INFORMATION

SET NO.: ONE

Pursuant to *California Code of Civil Procedure Section 2031.010 et seq.*, Plaintiff, John Smith, hereby demands that Defendant Mary Jones Enterprises, Inc., produce for inspection and copying all of the documents and electronically stored information within Defendant's possession, custody, or control as called for below, within the time required by statute. In addition, Plaintiff demands that the materials produced be organized and labeled to correspond with the categories in this set of demands.

The materials to be produced shall be produced at the offices of Tom Doe, Plaintiff's counsel, within 30 days after service of this set of demands. A personal appearance is not required if Defendant produces copies of all of the original materials, together with a verification under penalty of perjury that the copies are true and correct copies of the originals, within 30 days after service of this set of demands.

DEFINITIONS

1. "PLAINTIFF" means Plaintiff John Smith and includes his attorney of record and any agents, employees, and or investigators retained by his attorney of record.
2. "PERSON" and/or "INDIVIDUAL" means, unless otherwise specified, any natural person, firm, entity, corporation, partnership, proprietorship, association, joint venture, other form of organization or arrangement, and government and government agency of every nature or type.
3. "YOU," "YOUR," "PRODUCING PARTY," and/or "DEFENDANT" means Defendant Mary Jones Enterprises, Inc., and any other PERSON representing it or acting on its behalf.
4. "ELECTRONIC STORAGE DEVICE" means any device capable of storing ESI for any period of time, including without limitation disks, including hard disks and floppy disks, CD-ROMs, DVDs, network servers, shared servers, computers, magnetic tape, back-up tape, voice mail, temporary files, telephones, and PDAs, whether currently on Defendant's premises or otherwise (e.g., at an employee's home or remote office).
5. "ESI" means "electronically stored information" as defined in *California Code of Civil Procedure Section 2016.020(e)*, and shall include, without limitation, any information, including files, documents, images, video, metadata or any combination thereof stored, created, or used on any ELECTRONIC STORAGE DEVICE, disk, tape (including backup tapes and other backup media), or other computer or digital storage medium, microfilm, microfiche, floppy, or any other storage or recording medium. ESI includes without limitation electronic mail messages, voice mail messages, instant messaging or IM, text messages, information stored on web pages or web servers, and database records.
6. "RELATE," or any variant thereof, including, but not limited to, the term "relating to," shall be understood to apply if the data or information evidences, mentions, constitutes, contains, summarizes, describes, concerns, refers to (directly or indirectly), supports, contradicts, addresses in any way or otherwise deals with the subject matter described in this set of demands in which the term "relate," or any variant thereof, appears.
7. "EVIDENCE" or any variant thereof, including, but not limited to, the term "evidencing," shall be understood to apply if the data or information directly or indirectly mentions, discusses, constitutes, concerns, supports, contradicts, refers to, or in any other way deals with the subject matter described in this set of demands in which the term appears.
8. "DOCUMENT" means a writing as defined by *Evidence Code Section 250*, and shall include, without limitation, the original (and absent the original then a copy thereof), all file copies and copies not identical to the original of any writing or record of every type, form, and description that is in the possession, custody, or control of the responding party, or which no longer is in the responding party's possession but of which the responding party still has knowledge, whether or not said writings or records are claimed to be privileged or otherwise immune from discovery including by way of illustration and not limitation, the following items: notes, correspondence, communications of any nature (including intra-company communications and correspondence), electronic mail messages, telegrams, cables, memoranda (including internal memoranda), notebooks of any nature, including laboratory and engineering reports; summaries, minutes and records of telephone conversations, personal conversations or interviews; diaries, routing slips or memoranda, reports (including tests and analysis reports), books, manuals, publications, invoices, specifications,

shipping papers, purchase orders, shop instrument output, plans, patterns, drawings, flow charts, schematics, diagrams, photographs of any nature, artists' drawings, sketches, blueprints, minutes or recordings of meetings and conferences, including lists of persons attending meetings or conferences; transcripts of oral testimony or statements; reports and/or summaries of interviews; reports and/or summaries of investigations; opinions or reports of consultants; opinions of counsel; forecasts; reports of patent searches; patent opinions, analyses or appraisals; agreements and contracts (including all modifications or revisions thereof); reports and/or summaries of negotiations; court papers, labels, tags, placards, fliers, counter cards, brochures, pamphlets, advertisements, advertising layouts, circulars, trade letters, press releases, and translations; presentations, including boards, transparencies, storybooks and/or scripts; drafts of original or preliminary notes on, and marginal comments appearing on, any DOCUMENTS; whether those writings or records are on paper, magnetic disk, tape or other computer or digital storage medium, microfilm, microfiche, floppy, or any other storage or recording medium.

9. "ANY" shall be understood to include and encompass "all." As used herein, the singular shall always include the plural and the present tense also shall include the past tense. The words "and" as well as "or" shall be construed disjunctively or conjunctively as necessary to bring within the scope of this demand all documents or things that might otherwise be construed to be outside its scope.

10. To the extent that the documents demanded herein are not produced as they are kept in the usual course of business, then as to each document produced, indicate the number or numbers of the demands below to which the document is responsive.

11. If any document demanded herein is withheld pursuant to any objection based upon privilege, identify each document for which the privilege is claimed and state:

- a. The type of document (letter, report, memoranda, etc.), including any title or identifying number thereon;
- b. Its date of origin or preparation;
- c. The name of its author or originator;
- d. The name of its addressees, if any;
- e. A brief summary of its substance; and
- f. A factual and legal basis upon which a privilege is claimed sufficient to permit the Court to adjudicate the validity of the claim.

If any document demanded to be produced herein was in your possession, custody, or control, but has since been disposed of, lost, discarded, destroyed, or otherwise has become unavailable within four years of the date of this set of demands, please identify which documents were destroyed and state further the identity of the person who ordered them destroyed and the reason for their destruction.

DEMAND FOR FORMAT OF PRODUCTION

12. Load Files. Except for ESI described in Paragraphs 13(b) and (c) below, ESI must be produced in electronic format, with files suitable for loading into a Concordance [*or specify other type of database*] litigation support database. The load files will define document breaks, attachments and other information identified below.

(a) **Document Cross-Reference File.** YOU should provide a cross-reference file that identifies the start and end of the

document, its attachments and its corresponding metadata.

(b) **Cross-Reference or Linking File.** YOU should also provide a cross-reference file that facilitates the linking of the produced image or native file with the litigation database. This cross-reference file will contain fields such as the unique document ID (i.e., BegBates) and the file path of the corresponding image or native file. YOU may provide this information either in a Concordance litigation database format or as a standard delimited ASCII text file.

13. Categories of Production of ESI. ESI will be produced as follows, depending on its classification.

(a) **Production of ESI As TIFF Images With Metadata and Extracted Text.** Documents created in standard office automation file formats (including but not limited to Microsoft Word or WordPerfect documents) and ESI that can practicably be converted into TIFF format will be produced as single-page TIFF Group IV images, with any available fielded metadata and text searchable information extracted from the native documents.

(i) **Bates Numbering.** The producing party will brand all TIFF images in the lower right-hand corner with its corresponding Bates number, using a consistent font type and size. The Bates number must not obscure any part of the underlying image.

(ii) **File Names.** Image file names will be identical to the corresponding bates numbered images, with a ".tif" file extension.

(iii) **Confidentiality Endorsements.** The producing party will brand any confidentiality or similar endorsements in a corner of the TIFF image. Those endorsements must be in a consistent font type and size, and must not obscure any part of the underlying image or Bates number.

(iv) **Production of Extracted Full Text.** The producing party will provide extracted full text (i.e., text extracted from ESI) for all material originating as ESI in a text file corresponding to a single page of a document. The full text file name will be composed of the Bates number of the associated document, with a ".txt" file extension. When a party is unable to produce extracted full text, it will provide an explanation of that inability with its document production.

(v) **Production of Metadata.** The producing party will provide the following metadata, as applicable, for all ESI: start Bates, end Bates, start attachment, end attachment, custodian or source, original file path, original file name, file type/file extension, MD-5 hash value, title, creation date, creation time, page count, last modification date, last modification time, and last saved by name.

(vi) **Metadata for E-Mail.** In addition to the metadata to be produced for all ESI, for all e-mail, the producing party will also produce the following as fielded metadata: subject, author, recipients, from, to, copyees, blind copyees, date sent, time sent, date received, time received, MD-5 hash value, attachment file name, begin attachment, and end attachment. Family relationships among e-mail and attachments will be maintained by ensuring that attachments immediately follow their parent e-mail, and setting the "begin attachment" and "end attachment" metadata fields appropriately.

(vii) **Explanation of Inability to Produce Metadata.** When a party is unable to produce metadata for a particular field, it will provide an explanation of that inability with its document production.

(viii) **Redaction.** If a file that originates in ESI needs to be redacted before production, the file will be rendered in TIFF, and the TIFF will be redacted and produced. However, to the extent that the text is searchable in the native format, the producing party will still provide searchable text for those portions of the document that have not been redacted.

(b) **Production of Native Format Documents That Are Impractical to Convert to TIFF.** ESI that is not practical to convert to TIFF may be produced using one of the two following methods, which method will be subject to meet and confer between the parties.

(i) **Spreadsheets That Are Impractical to Convert to TIFF.** ESI that is not practical to convert to TIFF (for example, spreadsheets) may be produced in electronic format suitable for loading to a litigation support database with links to the native files.

(A) **Identification.** ESI produced in native file format will be assigned a unique DocID number within the litigation database.

(B) **File Names.** File names will be identical to the DocID number, followed by the original file name and file extension.

(C) **Authentication.** The producing party will provide a litigation database load file with separately fielded data, which will contain, as one of the fields, the MD-5 hash value of each file produced in native format.

(ii) **ESI That Is Impractical to Produce With Links to a Database.** For any ESI where linking a native document will render the document unusable, the ESI should be produced in native form, accompanied with a Bates number and MD-5 hash value, but separate from a litigation support database.

(iii) **Encrypted or Password-Protected ESI.** For any ESI that exists in encrypted format or is password-protected, the producing party will provide the propounding party a means to gain access to those native files (for example, by supplying passwords).

(c) **Reports in Lieu of Native Production.** If a party believes that it would be impractical to produce ESI in native format because of complexities associated with certain scheduling programs (such as Primavera), accounting systems, mapping systems, and/or other databases (such as MS Access, Oracle, and Microsoft SQL Server), it will so notify the propounding party and will inform the propounding party whether it has generated reports in the normal course of business using those programs or systems. In any such instance, the parties will meet and confer concerning the manner of production of those reports.

(d) **Production of Pictures/Images.** Any photographic images created and/or maintained in electronic format will be produced in that format.

14. **Production Media.** The producing party will use the appropriate electronic media (CD, DVD, or hard drive) for its ESI production, and will cooperate in good faith to use the highest capacity available media to minimize associated overhead. The producing party will label the physical media with the producing party, production date, media volume name, and document number range.

15. **Avoidance of Duplicate Production.** Each producing party will take all reasonable steps to reduce duplication of ESI. De-duplication will be performed within a custodian. The producing party will maintain references to all removed duplicate files.

16. **ESI Requiring Proprietary Software.** If proprietary software unavailable to PLAINTIFF is needed to review the producing party's ESI in native format, YOU shall provide reasonable access to the proprietary software for purposes of review of ESI by PLAINTIFF and any expert or other PERSON working on behalf of PLAINTIFF.

17. Translation of Data Compilations. If you contend that any ESI sought by these requests is subject to *California Code of Civil Procedure Section 2031.280(e)* providing for translation of data compilations through detecting devices at the reasonable expense of the demanding party, you should identify such ESI before any translation occurs, including without limitation explaining with specificity why you assert that section 2031.280(e) applies and what the reasonable expense of translation will be.

DEMAND FOR PRODUCTION NO. 1:

Documents and ESI related to Plaintiff's entire personnel file, covering the entire time that Plaintiff was employed by Defendant, including any of the following:

- Plaintiff's employment application.
- Plaintiff's discipline record.
- Plaintiff's performance evaluations.
- Plaintiff's salary and benefit history.

DEMAND FOR PRODUCTION NO. 2:

Documents and ESI relating to communications between Plaintiff and _____ [name], his/her supervisor during Plaintiff's employment with Defendant, relating to safety procedures at, or accidents or injuries occurring at, Defendant's rocket-engine testing facility located at _____ [address].

DEMAND FOR PRODUCTION NO. 3:

Documents and ESI relating to or evidencing communications between Plaintiff and the California Division of Occupational Safety and Health, or any official or employee of the California Division of Occupational Safety and Health, relating to safety procedures at, or accidents or injuries occurring at, Defendant's rocket-engine testing facility located at _____ [address].

DEMAND FOR PRODUCTION NO. 4:

Documents and ESI relating to or evidencing communications occurring on or after _____ [date] between or among Defendant, or any agent or employee of Defendant (including Plaintiff), and the California Division of Occupational Safety and Health, or any official or employee of the California Division of Occupational Safety and Health, relating to any aspect of Defendant's operations at its rocket-engine testing facility located at _____ [address].

DEMAND FOR PRODUCTION NO. 5:

Documents and ESI relating to or evidencing communications occurring on or after _____ [date] between or among any of Defendant's management personnel, including _____ [name], Plaintiff's supervisor, and any of Defendant's Human Resources management or staff, or between or among any combination of those persons, relating to any of the following:

- Plaintiff's job performance.
- Plaintiff's complaints about safety procedures at Defendant's rocket-engine testing facility located at

_____ [address].

■ Any contact or communication between Plaintiff and the California Division of Occupational Safety and Health.

■ Any contact or communication between Defendant, or any of its management, agents, or employees, and the California Division of Occupational Safety and Health, relating to safety procedures at, or accidents or injuries occurring at, Defendant's rocket-engine testing facility located at _____ [address].

DEMAND FOR PRODUCTION NO. 6:

Documents and ESI relating to or evidencing communications occurring on or after _____ [date] between or among any employees of Defendant, including Defendant's management personnel, relating to safety procedures at, or accidents or injuries occurring at, Defendant's rocket-engine testing facility located at _____ [address].

DEMAND FOR PRODUCTION NO. 7:

Documents and ESI relating to scheduled and periodic safety inspections conducted by Defendant on or after _____ [date] at its rocket-engine testing facility located at _____ [address].

DEMAND FOR PRODUCTION NO. 8:

Documents and ESI relating to employee accidents or injuries occurring on or after _____ [date] at Defendant's rocket-engine testing facility located at _____ [address], including any compilations of statistical data and reports prepared by or for Defendant.

DEMAND FOR PRODUCTION NO. 9:

Documents and ESI relating to Defendant's Workplace Injury and Illness Prevention Program for Defendant's rocket-engine testing facility located at _____ [address], including all revisions or suggested revisions to that program since it was adopted, and including any statistical reports and data analyses performed by or for Defendant, and any recommendations concerning the program made by any employee of Defendant, any consultant retained by Defendant, or any governmental agency.

DEMAND FOR PRODUCTION NO. 10:

Documents and ESI relating to instances in which Defendant, on or after _____ [date], terminated any of its employees, or disciplined an employee in any way, for _____ [specify].

DEMAND FOR PRODUCTION NO. 11:

Documents and ESI that support or relate to Defendant's answer to Interrogatory No. 5 of Plaintiff's First Set of Interrogatories to Defendant in this action, or that were reviewed, relied upon, or used in any way in answering that interrogatory by _____ [name of person who verified interrogatory answers] or any other person involved in preparing the answer to that interrogatory, including any compilations of statistical data and reports prepared by or for Defendant.

DEMAND FOR PRODUCTION NO. 12:

Documents and ESI that relate to or support Defendant's denial of the allegations of Paragraph 7 of the Complaint in this action, including any compilations of statistical data and reports prepared by or for Defendant.

Dated: _____
_____ [signature]

Tom Doe
Attorney for Plaintiff, John Smith

NOTES:

Authority:

CCP § 2031.010

Checklists:

See 6.03, 6.09

Discussion:

See 6.07, 6.11

Related Form--Demand for Inspection:

See 6.21



73 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 6 Demanding Production of Electronically Stored Information in California Court
V. FORMS*1-6 MB Practice Guide: CA E-Discovery and Evidence 6.21***6.21 Sample Demand for Inspection.**

Sample Demand for Inspection.

Tom Doe

California Bar Number 987654

California Bar Number 987654

100 North Main St., Suite 200

Farallon City, California 90000

Phone: 555-555-5555

Attorney for Plaintiff, John Smith

SUPERIOR COURT OF CALIFORNIA,

COUNTY OF FARALLON

John Smith,

Plaintiff, vs. Mary Jones Enterprises, Inc.,

Defendant.

)

)

)

)

)

No. _____

PLAINTIFF'S FIRST

DEMAND FOR INSPECTION

DEMANDING PARTY: PLAINTIFF, JOHN SMITH

RESPONDING PARTY: DEFENDANT, MARY JONES ENTERPRISES, INC.

SET NO.: ONE

To Defendant, Mary Jones Enterprises, Inc., and its attorney of record:

Pursuant to *California Code of Civil Procedure Section 2031.010 et seq.*, Plaintiff, John Smith, hereby demands that Defendant Mary Jones Enterprises, Inc., produce for inspection all items within Defendant's possession, custody, or control as called for below, within the time permitted by statute.

The items identified below shall be produced to allow full-disk forensic imaging and data preservation by _____ [name of forensic expert who will copy image] at the offices of Tom Doe, Plaintiff's counsel, within 30 days after service of this demand, unless counsel for the parties agree to set a different time or place for

production. The images of the items will be held by _____ until the parties agree on a protocol for review of the materials, or until order of the court.

DEMANDS FOR INSPECTION

DEMAND NO. 1:

Any computer (laptop and/or desktop) and other electronic storage devices, including but not limited to external hard drives, Zip drives, memory sticks, jump drives, USB/flashdrive devices, CDs, DVDs, floppy disks, e-mail accounts, Blackberries, other PDAs or cell phones with text messaging or electronic mail capabilities used by Defendant's employee, James Jones, during the period between May 2009 and the filing of the complaint in this action in November 2009.

Dated: _____
_____ [signature]

Tom Doe
Attorney for Plaintiff, John Smith

NOTES:

Authority:

CCP § 2031.010

Checklists:

See 6.03, 6.09

Discussion:

See 6.08[2], 6.11

Related Form--Demand for Production:

See 6.20



74 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 6 Demanding Production of Electronically Stored Information in California Court
V. FORMS

1-6 MB Practice Guide: CA E-Discovery and Evidence 6.22

6.22 Subpoena Duces Tecum (Judicial Council Form SUBP-010).

6.22.1 Subpoena Duces Tecum (Judicial Council Form SUBP-010).

[Click here to view image.](#)

ATTACHMENT 3

DEPOSITION SUBPOENA FOR PRODUCTION OF BUSINESS RECORDS TO FRANK COLE, CPA

DEFINITIONS

1. The terms "DOCUMENT," "DOCUMENTS," "WRITING," or "WRITINGS" mean a writing or writings as defined by *Evidence Code Section 250*, and shall include, without limitation, the original (and absent the original, then a copy thereof), all file copies and copies not identical to the original of any writing or record of every type, form, and description that is in the possession, custody, or control of the responding party, or which no longer is in the responding party's possession but of which the responding party still has knowledge, whether or not those writings or records are claimed to be privileged or otherwise immune from discovery, including, by way of illustration and not limitation, the following items: notes, correspondence, communications of any nature (including intra-company communications and correspondence), electronic mail messages, telegrams, cables, memoranda (including internal memoranda), notebooks of any nature, including laboratory and engineering reports; summaries, minutes and records of telephone conversations, personal conversations or interviews; diaries, routing slips or memoranda, reports (including tests and analysis reports), books, manuals, publications, invoices, specifications, shipping papers, purchase orders, shop instrument output, plans, patterns, drawings, flow charts, schematics, diagrams, photographs of any nature, artists' drawings, sketches, blueprints, minutes or recordings of meetings and conferences, including lists of persons attending meetings or conferences; transcripts of oral testimony or statements; reports and/or summaries of interviews; reports and/or summaries of investigations; opinions or reports of consultants; opinions of counsel; forecasts; reports of patent

searches; patent opinions, analyses or appraisals; agreements and contracts (including all modifications or revisions thereof); reports and/or summaries of negotiations; court papers, labels, tags, placards, fliers, counter cards, brochures, pamphlets, advertisements, advertising layouts, circulars, trade letters, press releases, and translations; presentations, including boards, transparencies, storybooks and/or scripts; drafts of original or preliminary notes on, and marginal comments appearing on, any DOCUMENTS; whether those writings or records are on paper, magnetic disk, tape or other computer or digital storage medium, microfilm, microfiche, floppy, or any other storage or recording medium.

2. "PLAINTIFF" means Plaintiff John Smith and includes his attorney of record and any agents, employees, and or investigators retained by his attorney of record.

3. "DEFENDANT" means Defendant Mary Jones Enterprises, Inc., and any of its predecessors and successors in interest, parents, subsidiaries, affiliates, segments, divisions, and operating units, and any of its present or former officers, partners, directors, administrators, agents, employees, consultants, investigators, accountants, attorneys, and all other persons acting or purporting to act on its behalf.

4. The terms "YOU" and "YOUR" shall mean Frank Cole, CPA, including nay of your affiliates, and any and all of your employees, partners, principals, members, directors, officers, employees, agents, representatives, accountants, financial advisors, investigators, consultants, attorneys, and any other person or entity acting on YOUR behalf.

5. "REFER" or "RELATE," or any variant thereof, including, but not limited to, the terms "REFERRING TO" and "RELATING TO," means in whole or in part evidencing, mentioning, constituting, containing, summarizing, describing, concerning, supporting, contradicting, addressing in any way, or otherwise dealing with the subject matter of the item listed below in which the term "REFER" or "RELATE" appears.

6. The term "COMMUNICATION(S)" shall be construed in the broadest possible sense and shall include, but not be limited to, any transmittal AND/OR receipt of information, whether by chance, prearranged, formal, or informal, and specifically includes conversations in person, telephone conversations, letters or memoranda, electronic mail, formal statements, press releases, AND newspaper articles.

7. The term "CORRESPONDENCE" means any exchange of COMMUNICATIONS, including without limitation memoranda, letters, electronic mail, messages sent or received from a wireless device, or other DOCUMENTS among individuals AND entities.

8. The terms "AND" and "OR" shall be construed disjunctively or conjunctively so as to bring within the scope of each item listed below all documents and things that might otherwise be construed to be outside its scope.

9. The singular shall include the plural, and vice versa, so as to make these requests broadly inclusive.

10. Each item listed below shall be construed independently and shall not be limited to reference to any other item.

11. If any document demanded herein is withheld pursuant to any objection based upon privilege, identify each document for which the privilege is claimed and state:

- a. The type of document (letter, report, memoranda, etc.), including any title or identifying number thereon;
- b. Its date of origin or preparation;
- c. The name of its author or originator;
- d. The name of its addressees, if any;

e. A brief summary of its substance; and

f. A factual and legal basis upon which a privilege is claimed sufficient to permit the Court to adjudicate the validity of the claim.

12. If any document demanded to be produced herein was in your possession, custody, or control, but has since been disposed of, lost, discarded, destroyed, or otherwise has become unavailable within four years of the date of this set of demands, please identify which documents were destroyed and state further the identity of the person who ordered them destroyed and the reason for their destruction.

13. Unless otherwise specified, each demanded item shall be produced in the form in which it is ordinarily maintained, preserving searchability, fielded metadata, and any files sent as e-mail attachments.

ITEMS TO BE PRODUCED

You are hereby required to produce all of the following documents that are now or were formerly in your possession, custody, or control (including documents at any time in the possession, custody, or control of your agents, attorneys, accountants, consultants, and all other persons and entities representing you or acting on your behalf):

1. Documents, including account statements, referring or relating to securities, investments, or money market accounts maintained for Defendant, for the period January 1, 2008, through December 31, 2009.

2. Communications between you and Defendant referring or relating to securities, investments, or money market accounts maintained for Defendant, for the period January 1, 2008, through December 31, 2009.

3. Documents referring or relating to any transfer of funds from Defendant's account no. 9362950304 at California International Bank to Plaintiff's account No. 8236452438 at Pacific State Bank made during the months of June, July, or August, 2009.

4. Communications between you and Defendant, made at any time, referring or relating to any of the transfers described in Item 3.

5. Communications between you and Plaintiff, made at any time, referring or relating to any of the transfers described in Item 3.

6. Federal and State corporate income tax returns for Defendant for any tax year ending in 2008 or 2009.

7. Documents referring or relating to any profit sharing plans, pension plans, Keogh plans, individual retirement accounts, stock ownership plans, 401(k) plans, and any other deferred compensation or retirement plans of any nature in which Plaintiff has or had any interest during the period from January 1, 2008 through the present.

NOTES:

Authority:

CCP § 1985.8

Checklist:

See 6.14

Discussion:

See 6.16, 6.17



75 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery

1-7 MB Practice Guide: CA E-Discovery and Evidence 7.syn

§ 7.syn Synopsis to Chapter 7: Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery

7.01 Scope.

7.02 Objective and Strategy.

7.03 CHECKLIST: Planning for Preservation of Electronic Evidence.

7.04 Options and Strategies.

7.05 Parties Have Duty To Preserve Electronic Evidence.

7.06 Reviewing Circumstances to Determine Whether Electronic Evidence Is at Risk of Destruction.

7.06[1] Ex Parte Order May Be Advisable If Party Fails to Comply With Duty to Preserve Electronic Evidence.

7.06[2] Likelihood of Inadvertent Loss or Destruction of Evidence May Make Injunction Advisable.

7.06[3] Possession or Access to Electronic Evidence by Nonparty May Make Injunction Advisable.

7.07 Assessing Availability of Court Order to Preserve Electronic Evidence.

7.07[1] Court Has Power to Issue Injunction Protecting Electronic Evidence.

7.07[1][a] Court Has Case Management Authority.

7.07[1][b] Court Has Statutory Authority to Enjoin Conduct That Would Render Judgment Ineffectual.

7.07[1][c] Court Has Inherent Power to Make Orders Facilitating Discovery.

7.07[2] Determining Whether Requirements for Injunctive Relief Are Met.

7.07[2][a] Traditional Factors Apply.

7.07[2][b] Court Must Assess Moving Party's Likelihood of Success on Merits.

7.07[2][c] Court Must Balance Relative Harms to Parties.

7.07[2][d] Party Seeking Injunction May Argue Inadequacy of Legal Remedies for Spoliation of Evidence.

7.07[3] Court May Issue Injunction Tailored to Circumstances of Case.

7.07[3][a] Court May Issue Nonspoliation Order.

7.07[3][b] Court May Issue Order Requiring Neutral Expert to Seize and Copy Electronic Evidence.

7.08 Weighing Advantages and Disadvantages of Seeking Order to Preserve Electronic Evidence.

7.08[1] Advantages and Disadvantages of Seeking Injunctive Order.

7.08[1][a] Ex Parte Order May Be Obtained on Short or No Notice on Showing of Great or Irreparable Injury.

7.08[1][b] If Showing Required for Ex Parte Order Cannot Be Made, Time and Cost Factors May Make Noticed Motion for Injunction Undesirable.

7.08[1][c] Applicant Must Provide Bond or Undertaking.

7.08[2] Alternative Approaches Should Be Considered.

7.09 CHECKLIST: Obtaining Injunction To Preserve Electronic Evidence.

7.10 Options and Strategies.

7.10[1] Decide Whether to Proceed Ex Parte.

7.10[2] Decide What Terms to Request in Injunctive Order.

7.11 Making Ex Parte Application for Temporary Restraining Order to Preserve Electronic Evidence.

7.11[1] Party Seeking Order Must Prepare Moving Papers.

7.11[1][a] Party Seeking Order Must Prepare Ex Parte Application.

7.11[1][b] Application Must Be Accompanied by Declarations Establishing Basis for Ex Parte Relief.

7.11[1][c] Application Must Be Accompanied by Declarations Establishing Basis for Injunction.

7.11[1][d] Application Must Be Accompanied by Declaration of Notice.

7.11[1][e] Application Must Be Accompanied by Supporting Memorandum.

7.11[1][f] Application Must Be Accompanied by Proposed Order.

7.11[2] Applicant Must Serve Notice of Ex Parte Application.

7.11[3] Ex Parte Application Should Be Presented to Court.

7.11[4] Applicant Must Appear Before Court Unless Parties Have Stipulated to Order.

7.11[5] Order Must Be Signed, Filed, and Served.

7.12 Making Noticed Motion for Preliminary Injunction to Preserve Electronic Evidence.

7.12[1] Party Seeking Order Must Prepare Moving Papers.

7.12[1][a] Party Seeking Order Must Prepare Notice of Motion and Motion.

7.12[1][b] Motion Must Be Accompanied by Supporting Declarations.

7.12[1][c] Motion Must Be Accompanied by Request for Judicial Notice If Notice Is Being Requested.

7.12[1][d] Party Seeking Permission to Present Oral Testimony Must File Written Statement.

7.12[1][e] Motion Must Be Accompanied by Supporting Memorandum.

7.12[1][f] Motion Must Be Accompanied by Proposed Order.

7.12[2] Moving Papers Must Be Filed in Clerk's Office.

7.12[3] Motion Must Be Served and Filed Within Applicable Time Limits.

7.12[4] Reply Memorandum Should Be Prepared in Response to Opposing Memorandum.

7.12[5] Counsel Should Attend Hearing on Motion.

7.12[6] Order Must Be Signed, Filed, and Served.

7.13 CHECKLIST: Opposing Injunction to Preserve Electronic Evidence.

7.14 Options and Strategies.

7.15 Opposing Application or Motion for Injunction to Preserve Electronic Evidence.

7.15[1] Preparing Opposing Papers.

7.15[1][a] Opposing Party Should Prepare Memorandum.

7.15[1][b] Opposing Party Should Prepare Declarations.

7.15[2] Filing and Serving Opposing Papers.

7.15[2][a] Opposing Party Must Serve Opposition to Ex Parte Application.

7.15[2][b] Opposing Party Must Serve Opposition to Noticed Motion.

- 7.16 Ex Parte Application for Temporary Restraining Order and Order to Show Cause.
- 7.17 Declaration in Support of Ex Parte Application for Temporary Restraining Order and Order to Show Cause.
- 7.18 Declaration Supporting Application or Motion for Injunctive Relief.
- 7.19 Order to Show Cause and Temporary Restraining Order Directing Preservation of Electronic Evidence.
- 7.20 Notice of Motion and Motion for Preliminary Injunction to Preserve Electronic Evidence.
- 7.21 Declaration Opposing Motion for Preliminary Injunction to Preserve Electronic Evidence.
- 7.22 Order--Preliminary Injunction Directing Preservation of Electronic Evidence.
- 7.23 Order--Preliminary Injunction Directing Seizure and Copying of Electronic Evidence.



76 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery

I. STRATEGY

1-7 MB Practice Guide: CA E-Discovery and Evidence 7.01

7.01 Scope.

This chapter covers:

- Planning for the preservation of electronic evidence pending discovery [see 7.03-7.08].
- Obtaining an injunction to preserve electronic evidence pending discovery [see 7.09-7.12; *Forms*: 7.16-7.20, 7.22, 7.23].
- Opposing an injunction to preserve electronic evidence pending discovery [see 7.13-7.15; *Form*: 7.21].

This chapter does not cover the use of specific discovery procedures to obtain the production of electronic evidence. For discussion of the procedure for requesting production of electronically stored information, see *Ch. 6, Demanding Production of Electronically Stored Information in California Court*, 6.03-6.13.

This chapter does not cover enforcement of injunctions. For coverage of enforcement, see *Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure*, *Ch. 18*, 18.19-18.21.

This chapter does not cover appeals from the grant or denial of preliminary injunctive relief. For coverage of appeals, see *Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure*, *Ch. 18*, 18.22-18.25.

Core Statutes:

CCP §§ 526, 527, 1005



77 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery

I. STRATEGY

1-7 MB Practice Guide: CA E-Discovery and Evidence 7.02

7.02 Objective and Strategy.

The objective of an injunction to preserve electronic evidence pending discovery is to ensure that relevant evidence is not inadvertently or intentionally deleted, lost, or destroyed before it can be produced through normal discovery channels. To accomplish this objective, counsel also should consider alternative procedures, including meeting and conferring with opposing counsel in an attempt to reach a stipulation regarding the preservation of electronic evidence [see *Cal Rules Ct, Rule 3.724(8)*].

Cross References:

Discussion of alternative strategies, see 7.08[2].

Discussion of meeting with opposing counsel to confer regarding discovery of electronically stored information, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferring, and Case Management Conference*, 5.14-5.25.



78 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery

II. PLANNING FOR PRESERVATION OF ELECTRONIC EVIDENCE

1-7 MB Practice Guide: CA E-Discovery and Evidence 7.03

7.03 CHECKLIST: Planning for Preservation of Electronic Evidence.

☐ Identify, as precisely as possible, electronically stored information that is likely to be sought in discovery, including following details:

- ☐ Specific information that is stored electronically and that client is likely to seek in discovery.
- ☐ Medium or form in which information is maintained.
- ☐ Custodian of electronically stored information, either party to litigation or third party.
- ☐ Custodian's regular procedures for creating, maintaining, backing up, copying, and deleting electronically stored information.
- ☐ Whether any copies of information are in existence and, if so, where, by whom, and in what form those copies are maintained.

☐ Determine whether information identified above is at risk of loss or destruction.

- ☐ Consider whether nature of relevant electronic evidence, or form in which it is maintained, carries substantial risk that evidence will be lost or destroyed before it can be produced in discovery, such as electronic information that is maintained for opposing party's current business operations and is subject to modification or deletion on ongoing basis.

Authority:

See, e.g., *Columbia Pictures Indus. v. Bunnell* (CD Cal May 29, 2007) 2007 US Dist LEXIS 46364, at *2-*4, *aff'd* 245 FRD 443 (CD Cal 2007) (ordering preservation of search data in RAM that was relevant but not maintained in the ordinary course of business)

Discussion:

See 7.06

- ☐ Consider whether opposing party's previous conduct, current refusal to agree to preserve electronic evidence, or other circumstances indicate that relevant electronic evidence might be destroyed intentionally.

Discussion:

See 7.06[1]

- ☐ If electronically stored information is at risk of loss or destruction, determine whether injunctive relief is available to preserve information.

- ☐ Determine whether client is likely to prevail on merits of discovery request for electronically stored information.

Authority:

CCP § 2017.010; *Dodge, Warren & Peters Ins. Servs., Inc. v. Riley* (2003) 105 CA4th 1414, 1420-1421, 130 CR2d 385

Discussion:

See 7.07[2][b]

- ☐ Ascertain that information is relevant or likely to lead to discovery of admissible evidence.

- ☐ Ascertain that information is not privileged or, alternatively, that any privileged information recovered can be later identified, segregated, and removed before production.

- ☐ Determine whether harm to client from nonissuance of injunctive relief would outweigh harm to adverse party or custodian of information from issuance of injunction.

Authority:

CCP § 526(a)(2), (3); *Dodge, Warren & Peters Ins. Servs., Inc. v. Riley* (2003) 105 CA4th 1414, 1421, 130 CR2d 385

Discussion:

See 7.07[2][c]

- ☐ Determine whether, if injunction is not issued and information is lost, damages or other legal remedy would not adequately compensate client.

Authority:

CCP § 526(a)(4); Dodge, Warren & Peters Ins. Servs., Inc. v. Riley (2003) 105 CA4th 1414, 1419, 130 CR2d 385

Discussion:

See 7.07[2][b]

☐ Consider what form of injunctive relief would best achieve client's objectives, such as:

☐ Nonspoliation order, enjoining adverse party or other custodian of information from destroying or deleting specific electronically stored information.

Discussion:

See 7.07[3][a]

Form:

See 7.22

☐ Order appointing independent expert to take possession of and copy specific electronically stored information.

Discussion:

See 7.07[3][b]

Form:

See 7.23

☐ Consider whether alternative order or procedure would effectively achieve client's objectives, such as:

Discussion:

See 7.08[2]

☐ Order shortening regular timetable for discovery of specific electronically stored information.

Authority:

CCP §§ 2031.020(b), (d), 2031.030(c)(2)

☐ Sending adverse party written notice that discovery of electronically stored information is reasonable likely to be sought, and then meeting and conferring with opposing counsel to arrive at agreement regarding preservation and discovery of that information.

Authority:

Cal Rules Ct, Rule 3.724(8)

☐ Asking court at case management conference to issue resolve issues pertaining to preservation and discovery of electronically stored information [see *Cal Rules Ct, Rule 3.728(13)*].

Authority:

Cal Rules Ct, Rule 3.728(13)



79 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery

II. PLANNING FOR PRESERVATION OF ELECTRONIC EVIDENCE

*1-7 MB Practice Guide: CA E-Discovery and Evidence 7.04***7.04 Options and Strategies.**

A litigant's ability to present his or her case can be seriously compromised by the loss or destruction--whether intentional or inadvertent--of relevant electronic evidence, whether that evidence is possessed by the litigant or is in the hands of an opposing party or a third party. Moreover, a litigant's destruction of electronic or other evidence in anticipation of or in response to a discovery request is a misuse of the discovery process that may subject the litigant to monetary sanctions, issue sanctions, evidence sanctions, contempt sanctions, and even dismissal of a claim or defense [see *Cedars-Sinai Med. Ctr. v. Superior Court* (1998) 18 C4th 1, 12, 74 CR2d 248, 954 P2d 511 ; CCP §§ 2023.010, 2023.030].

 Cross Reference:

Seeking or opposing sanctions, see Ch. 13, Seeking or Opposing Sanctions for Noncompliance.

Therefore, even before litigation commences, counsel should advise the client to implement procedures to preserve the client's own relevant electronic evidence. Then, early in the litigation, counsel should take steps to (1) prevent the opposing party from destroying relevant electronic evidence that will be sought through discovery, and (2) prevent the loss of electronic evidence that is in the possession of third parties.

 Cross References:

Planning for discovery of electronic evidence, see Ch. 4, Planning E-Discovery, 4.03-4.10.

Notifying client of importance of preserving electronic evidence, see *Ch 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference*, 5.03-5.08

Best practices for retention of electronically stored information, see Ch. 16, Establishing Best Practices Regarding Electronically Stored Information.

Strategic Points:

As early as possible in the litigation process, counsel should inform opposing counsel in writing that discovery of electronically stored information is reasonably likely to be sought [see *Cal Rules Ct, Rule*

3.724(8)]. If possible, counsel should strive to reach a stipulation with opposing counsel regarding the preservation of electronic evidence. Early notice that electronic evidence will be sought is especially important if the relevant electronic evidence is kept as part of the opposing party's current business operations and thus is subject to being modified or deleted as part of the party's regular operations. Documentation that the opposing party has been put on notice of the need to preserve the electronic evidence may be useful should it later become necessary to seek sanctions for the destruction or spoliation of the evidence.



Timing--Plaintiff:

Unless a party receives leave of court (for example, with the grant of an order allowing expedited discovery), a plaintiff must wait 10 days after service of the summons before serving a demand for inspection, copying, testing, or sampling of electronically stored information [CCP § 2031.020(b)]. However, this 10-day waiting period does not apply to a notice that discovery of electronically stored information is reasonably likely to be sought [see *Cal Rules Ct, Rule 3.724*]. Therefore, if there is any possibility of intentional or inadvertent loss or destruction of the electronic evidence in the hands of the defendant, the better practice is to serve a notice that discovery of electronically stored information is reasonably likely to be sought along with the summons and complaint.



Cross Reference:

Notice that discovery of electronically stored information is reasonably likely to be sought, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference, 5.09-5.13*.

Discussion of expedited discovery orders, see 7.10[2]

If the parties cannot come to an agreement regarding the preservation of electronic evidence, counsel should consider seeking an injunction to protect relevant electronic evidence pending discovery [see *Dodge, Warren & Peters Ins. Servs., Inc. v. Riley (2003) 105 CA4th 1414, 1418-1421, 130 CR2d 385*].



Cross References:

Checklist for obtaining injunction, see 7.09.

Form for noticed motion for injunction, see 7.20.



Strategic Point:

If counsel believes that the opposing party will react to notice of planned electronic discovery by trying to destroy damaging evidence, counsel should forgo such notice and consider seeking a temporary restraining order ex parte.



Cross Reference:

Form for ex parte application for temporary restraining order, see 7.16.



80 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery

II. PLANNING FOR PRESERVATION OF ELECTRONIC EVIDENCE

1-7 MB Practice Guide: CA E-Discovery and Evidence 7.05

7.05 Parties Have Duty To Preserve Electronic Evidence.

If a party knows or should know that it possesses electronically stored information that is or might be relevant to litigation, the party has a duty to preserve that information [see *UMG Recordings, Inc. v. Hummer Winblad Venture Partners (In re Napster, Inc. Copyright Litig.)* (ND Cal 2006) 462 F Supp 2d 1060, 1069] ; *Zubulake v. UBS Warburg LLC* (SDNY 2003) 220 FRD 212, 216 ; *Cedars-Sinai Med. Ctr. v. Superior Court* (1998) 18 C4th 1, 12, 74 CR2d 248, 954 P2d 511 ; *Dodge, Warren & Peters Ins. Servs., Inc. v. Riley* (2003) 105 CA4th 1414, 1418-1420, 130 CR2d 385] . This duty to preserve electronic evidence may require placing a "litigation hold" on the party's routine procedures for retention or destruction of electronic documents [see *Cedars-Sinai Med. Ctr. v. Superior Court* (1998) 18 C4th 1, 12, 74 CR2d 248, 954 P2d 511 ("a lawyer customarily instructs the client to preserve and maintain any potentially relevant evidence"); *Thompson v. United States HUD* (D Md 2003) 219 FRD 93, 100-105 (noting ethical obligations for attorneys to preserve evidence)].

The duty to preserve relevant electronic evidence also may include the obligation to inform the opposing party of the possibility of destruction or loss of electronic evidence that is in the possession or control of another person [see *Silvestri v. GMC* (4th Cir. 2001) 271 F3d 583, 591] .

**Warning--Party Must Protect the Evidence It Seeks to Preserve:**

A party who seeks protection for electronic evidence in the possession of another party or a third party is expected to take steps to assure that the evidence is preserved. California does not recognize a tort of spoliation of tangible evidence and usually will not allow after-the-fact litigation over spoliation of evidence, relying instead on the substantial protection and deterrent afforded to the parties by the evidentiary inferences of *Evid Code* § 413 and the discovery remedies of *CCP* § 2023.030 [see *Coprich v. Superior Court* (2000) 80 CA 4th 1081, 1089-1090, 95 CR2d 884 ; *Cedars-Sinai Medical Center v. Superior Court* (1998) 18 C4th 1, 74 CR2d 248 , 954 P2d 511 ; *Temple Cmty. Hosp. v. Superior Court* (1999) 20 C4th 464, 476-478, 84 CR2d 852, 976 P2d 223] .

**Cross Reference:**

Discussion of obligation to preserve electronic evidence, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference, 5.05.*



81 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery

II. PLANNING FOR PRESERVATION OF ELECTRONIC EVIDENCE

*1-7 MB Practice Guide: CA E-Discovery and Evidence 7.06***7.06 Reviewing Circumstances to Determine Whether Electronic Evidence Is at Risk of Destruction.**

7.06[1] Ex Parte Order May Be Advisable If Party Fails to Comply With Duty to Preserve Electronic Evidence. If counsel becomes aware of any facts indicating that an adverse party in possession of electronic evidence is likely to delete, destroy, or alter any portion of that evidence, or has done so in the past, counsel should seriously consider seeking an ex parte temporary restraining order against such conduct.

Example:

An adverse party's complete refusal to consider entering into any agreement regarding the preservation of electronic or other evidence might be an indication that such evidence is at risk of deletion, destruction, or alteration before discovery can be had.

**Cross Reference:**

Discussion of obtaining ex parte restraining order, see 7.11.

7.06[2] Likelihood of Inadvertent Loss or Destruction of Evidence May Make Injunction Advisable.

Electronic evidence may be inadvertently deleted or destroyed in the ordinary course of business. For example, a computer user might delete potentially relevant files to create more storage space, or a computer maintenance program might routinely remove old files [see, e.g., *Columbia Pictures Indus. v. Bunnell* (CD Cal May 29, 2007) 2007 US Dist LEXIS 46364, 2-4, *aff'd* 245 FRD 443 (CD Cal 2007) (user search data in RAM would be written over absent preservation order); *Creative Sci. Sys. v. Forex Capital Mkts., LLC* (ND Cal April 4, 2006) 2006 US Dist LEXIS 20116 (data lost due to installing operating systems)].

**Warning--Backups Do Not Guarantee Availability of Desired Information:**

The existence of a computer backup procedure does not necessarily guarantee that relevant information will always be available. If a party routinely "backs up," or makes copies of, information on its computer system, then information that has been deleted from the main computer system may remain available on the backup media. However, the backup copies of the information might eventually be overwritten or destroyed if backup files are reused for more current system backups. Thus, if older backup media are reused, as they frequently are, potentially relevant data may eventually be lost unless the party takes steps to preserve its backup copies.



Strategic Point--Recoverability of Deleted Files:

Counsel should not assume that deleted computer files are lost forever. Although a file or document on a computer can be deleted or erased by means of the delete function, such information may continue to exist in electronic form on the computer's hard drive until overwritten with new data. Thus, electronic information that has been deleted has not necessarily been destroyed and might, under some circumstances, still be recovered [see, e.g., *Antioch Co. v. Scrapbook Borders, Inc.* (D Minn 2002) 210 FRD 645, 651-654 (granting motion to appoint expert to attempt to resurrect data that had been deleted from defendants' computer equipment); *Playboy Enters. v. Welles* (SD Cal 1999) 60 F Supp 2d 1050, 1052-1055 (in trademark suit, e-mails were missing and had been deleted; plaintiff asked for mirror image of computer to retrieve); *Gates Rubber Co. v. Bando Chem. Indus.* (D Colo 1996) 167 FRD 90, 112-113 (discussing procedures for recovery of fragments of deleted files)].



Cross Reference:

Recovery of deleted files, see *Ch. 1, Understanding Electronic Evidence*, 1.22[6], 1.38, 1.40[2].



Warning--Limitations on Court's Power to Impose Sanctions:

Absent exceptional circumstances, the court has no power to impose sanctions on a party or any attorney for a party for a failure to provide discovery of electronically stored information that has been lost, damaged, altered, or overwritten as a result of the routine, good-faith operation of an electronic information system [CCP §§ 2031.060(i)(1), 2031.300(d)(1), 2031.320(d)(1)]. 2031.310(j)(1), 2031.320(d)(1)]. Thus, if such a loss of evidence occurs, an adverse party whose case depends on the lost evidence may have no recourse. Accordingly, it is imperative that counsel take steps as early as possible to ensure the preservation of electronic evidence in the hands of another party [see *Cedars-Sinai Medical Center v. Superior Court* (1988) 18 Cal. 4th 1, 74 CR2d 248, 954 P2d 511 ; *Temple Cmty. Hosp. v. Superior Court* (1999) 20 Cal. 4th 464, 476-478, 84 CR2d 852, 976 P2d 223 (refusing to create a tort remedy for spoliation and observing that a party must take active steps to ensure that evidence is preserved)].

7.06[3] Possession or Access to Electronic Evidence by Nonparty May Make Injunction Advisable. Absent exceptional circumstances, the court has no power to impose sanctions on a subpoenaed nonparty or any attorney for a subpoenaed person for a failure to provide discovery of electronically stored information that has been lost, damaged, altered, or overwritten as a result of the routine, good-faith operation of an electronic information system [CCP § 1985.8(l)(1)]; but see *Temple Cmty. Hosp. v. Superior Court* (1999) 20 Cal. 4th 464, 476-478, 84 CR2d 852, 976 P2d 223 (discussion of other remedies potentially available for loss of evidence), discussed in 7.08[2]]. Thus, if such a loss of evidence occurs, a party whose case depends on the lost evidence may have no recourse. Accordingly, it is imperative that counsel take steps as early as possible to ensure the preservation of electronic evidence in the hands of nonparties.



Cross Reference:

Discussion of discovery of electronically stored information from nonparty, see *Ch. 6, Demanding Production of Electronically Stored Information in California Court*, 6.14-6.19.



82 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery

II. PLANNING FOR PRESERVATION OF ELECTRONIC EVIDENCE

1-7 MB Practice Guide: CA E-Discovery and Evidence 7.07

7.07 Assessing Availability of Court Order to Preserve Electronic Evidence.

7.07[1] Court Has Power to Issue Injunction Protecting Electronic Evidence.

7.07[1][a] Court Has Case Management Authority. A court's case management authority includes the power to make any orders that may be appropriate, including orders on matters relating to discovery or electronically stored information [*Cal Rules Ct, Rule 3.728(13), (14); see Cal Rules Ct, Rule 3.724(8)*].

7.07[1][b] Court Has Statutory Authority to Enjoin Conduct That Would Render Judgment Ineffectual. A court may grant a preliminary injunction when it appears that a party to the action is doing, is threatening, is about to do, or is procuring or suffering to be done some act in violation of another party's rights that would tend to render the eventual judgment ineffectual [*CCP § 526(a)(3)*]. This general statutory principle applies when the eventual "judgment" will consist of a decision about a party's right to discovery. Thus, a court may issue a preliminary injunction to preserve electronic evidence whenever a party's conduct while a discovery request is pending may result in the loss of the evidence, rendering any discovery order ineffectual [*Dodge, Warren & Peters Ins. Servs., Inc. v. Riley (2003) 105 CA4th 1414, 1418-1419, 130 CR2d 385*] .

Prerequisite:

Prerequisite: The court's power to issue an injunctive order protecting electronic evidence is triggered by a party's actual or potential conduct that may result in the loss or destruction of the evidence, even if that conduct is innocent [*Dodge, Warren & Peters Ins. Servs., Inc. v. Riley (2003) 105 CA4th 1414, 1418-1419, 130 CR2d 385*] .

7.07[1][c] Court Has Inherent Power to Make Orders Facilitating Discovery. A trial court has broad discretion to ensure the effective administration of justice. This includes the inherent power to make orders facilitating discovery and the presentation of evidence, such as a preliminary injunction to preserve electronic evidence pending discovery [*Dodge, Warren & Peters Ins. Servs., Inc. v. Riley (2003) 105 CA4th 1414, 1418-1419, 130 CR2d 385* ; *Northpoint Homeowners Assn. v. Superior Court (1979) 95 CA3d 241, 244, 157 CR 42* ; *see Pueblo of Laguna v. United States (2004) 60 Fed Cl 133, 135* (courts' inherent powers include ability to order evidence preserved)].

7.07[2] Determining Whether Requirements for Injunctive Relief Are Met.

7.07[2][a] Traditional Factors Apply. Trial courts traditionally consider and weigh two factors in determining

whether to issue a preliminary injunction, and those factors are applicable in the context of a preliminary injunction to preserve evidence [*Dodge, Warren & Peters Ins. Servs., Inc. v. Riley (2003) 105 CA4th 1414, 1420, 130 CR2d 385*] :

- First, whether the moving party is likely to prevail on the merits. In this context, that means the court must consider whether the party seeking an injunction to preserve electronic evidence is likely to establish that the evidence is discoverable.
- Second, the balance of relative harms the parties will suffer in the interim due to the issuance or nonissuance of the injunction.

In addition, as a prerequisite to the issuance of any equitable relief, including a preliminary injunction, the moving party must establish that any legal remedy for the potential wrong (i.e., the destruction of the evidence) is inadequate or unavailable [*Dodge, Warren & Peters Ins. Servs., Inc. v. Riley (2003) 105 CA4th 1414, 1419-1420, 130 CR2d 385*] .

Cross References:

Discussion of moving party's likelihood of success, see 7.07[2][b].

Discussion of balance of harms, see 7.07[2][c].

Discussion of establishing inadequacy of legal remedy, see 7.07[2][d].

7.07[2][b] Court Must Assess Moving Party's Likelihood of Success on Merits. The trial court first must determine whether the moving party is likely to prevail on the merits. In the context of a motion for a preliminary injunction to preserve electronic evidence pending discovery, the court's inquiry into whether the moving party is likely to prevail on the merits concerns the merits of the question of discoverability of the evidence [*Dodge, Warren & Peters Ins. Servs., Inc. v. Riley (2003) 105 CA4th 1414, 1420-1421, 130 CR2d 385*] .



Strategic Point--Moving Party:

The requisite showing of a likelihood of success by the moving party usually is not difficult, since discovery traditionally has been liberally granted by the courts. The Discovery Act authorizes inquiry into even irrelevant matters as long as their revelation may lead to the discovery of admissible evidence [*Dodge, Warren & Peters Ins. Servs., Inc. v. Riley (2003) 105 CA4th 1414, 1420, 130 CR2d 385* ; see CCP § 2017.010].

Example:

An insurance brokerage firm sued its former employees, claiming misappropriation of trade secrets, unfair business practices, breach of fiduciary duty, and breach of contract. The plaintiff sought a preliminary injunction to preserve electronically stored information copied by the defendants from the plaintiff's computers. The record established that the defendants had copied many of the plaintiff's computer files onto discs and took them off-site for later use in competing with the plaintiff. The defendants admitted having taken voluminous files from the plaintiff, and the record indicated that the defendants' computers might also contain other evidence supportive of the plaintiff's causes of action. Under the circumstances, given the traditionally liberal discovery standard, the court of appeal found that the trial court had not abused its discretion in determining that the defendants' computer and electronic storage media contained information that the plaintiff would have a right to discover [*Dodge, Warren & Peters Ins. Servs., Inc. v. Riley (2003) 105 CA4th 1414, 1420-1421, 130 CR2d 385*] .



Strategic Point--Opposing Party:

Although discovery has traditionally been liberally granted by the courts, it may be possible for the party opposing a motion for a preliminary injunction to show that the moving party is not likely to succeed in establishing that the information is discoverable. This may be done by showing either (1) that the information sought is privileged, or (2) that the information sought is not admissible and is not likely to lead to the discovery of admissible evidence [see CCP § 2017.010; *Dodge, Warren & Peters Ins. Servs., Inc. v. Riley* (2003) 105 CA4th 1414, 1421, 130 CR2d 385] .

7.07[2][c] Court Must Balance Relative Harms to Parties. The court must balance the relative harms the parties will suffer in the interim due to the issuance or nonissuance of the injunction [see *Columbia Pictures Indus. v. Bunnell* (CD Cal May 29, 2007) 2007 US Dist LEXIS 46364, at *28-*29 , *aff'd* 245 FRD 443 (CD Cal 2007) (court must consider any irreparable harm to moving party absent preservation order as well as capability of burdens on responding party of maintaining evidence, including physical, spatial, and financial burdens created by ordering evidence preservation)]. The balance of harms ordinarily will favor the party seeking to preserve electronically stored information, if the loss of the information would significantly hinder that party's ability to present its case, and the preservation of the information would not affect the responding party's ability to conduct its business [see *Dodge, Warren & Peters Ins. Servs., Inc. v. Riley* (2003) 105 CA4th 1414, 1421, 130 CR2d 385] .

Example:

An insurance brokerage firm sued its former employees, claiming misappropriation of trade secrets, unfair business practices, breach of fiduciary duty, and breach of contract. After the trial court issued a preliminary injunction to preserve electronically stored information copied by the defendants from the plaintiff's computers, the court of appeal affirmed. On the issue of the relative harms, the court of appeal noted that the record indicated that in the absence of an order to preserve the information, the plaintiff could have irretrievably lost evidence that otherwise would have been available to it. On the other hand, the record showed that the harm to the defendants resulting from the issuance of the injunction was negligible. Under the terms of the trial court's injunction, copying of the information would be done in the defendants' presence and after working hours so as not to interrupt their ability to conduct business, and no damage to or loss of information would result from the copying. In addition, the copied material would be unavailable to anyone except upon agreement of the parties or order of the court; thus, concerns over privacy and privilege were minimized to the point of nonexistence. Further, the reasonable cost to defendants to review the copied files for irrelevant and privileged documents was to be borne by the plaintiff, subject to reallocation by the trial court. Under those circumstances the court of appeal concluded that the trial court had not abused its discretion in determining that the plaintiff would have suffered greater harm in the absence of an injunction than the defendants would suffer from the issuance of the injunction [*Dodge, Warren & Peters Ins. Servs., Inc. v. Riley* (2003) 105 CA4th 1414, 1421, 130 CR2d 385] .



Strategic Points--Moving Party--Responses to Assertion that Injunction Would Be Unduly

Burdensome:

The opposing party may assert that an order to preserve a copy (sometimes called a "mirror image") of information stored on its computer equipment would be unduly burdensome because of the expense involved. In such a case, the moving party should be willing to pay the cost of creating a copy of the electronically stored information [see *Playboy Enters. v. Welles* (SD Cal 1999) 60 F Supp 2d 1050, 1055 n6] .

The opposing party also may assert that creating a mirror image would be unduly burdensome and

intrusive because confidential and privileged information would be swept up along with potentially discoverable material. In such a case, the moving party should suggest that the court appoint a neutral computer expert to serve as an officer of the court in creating a mirror-image copy of the electronically stored information. The expert's status as an officer of the court would prevent his or her access to the copied information from being treated as a waiver of any claim of confidentiality or privilege [see *Playboy Enters. v. Welles* (SD Cal 1999) 60 F Supp 2d 1050, 1055 ; *Simon Prop. Group L.P. v. MySimon, Inc.* (SD Ind 2000) 194 FRD 639, 642] . The moving party should also suggest that the court order that the expert give the mirror-image copy of the information to the opposing party's counsel, who will be the sole custodian of the mirror image throughout the litigation. The opposing party's counsel then can print and review any recovered documents and produce those documents that are responsive to discovery requests. The opposing party's counsel can also create a privilege log of any documents that are withheld on a claim of privilege, and the privilege log can be used for in camera review by the court if any claim of privilege is disputed [*Playboy Enters. v. Welles* (SD Cal 1999) 60 F Supp 2d 1050, 1055] . Alternatively, the court may order the expert to provide the court with a full copy of the mirror image, to be reviewed in camera in the event of discovery disputes [*Antioch Co. v. Scrapbook Borders, Inc.* (D Minn 2002) 210 FRD 645, 653-654] .

Example:

In a trademark infringement action in federal court, the court found it likely that relevant information was stored on the hard drive of the defendant's computer, in the form of deleted e-mails. The court found that the plaintiff's need for the information outweighed the burden on the defendant's business operations of allowing access to her computer, provided that the plaintiff could provide evidence that recovering some of the deleted e-mails was at least as likely as not recovering any of the e-mails, and that no damage would be done to the defendant's computer in the recovery process. If such evidence could be provided, the court stated that it would appoint a computer expert to create a "mirror image" of the defendant's hard drive. The court dealt with possibility that confidential and privileged information would be included in the mirror image as follows. First, the court would appoint the expert to serve as an officer of the court, so that allowing the expert access to the hard drive would not constitute a waiver by the defendant of privilege as to any information on the hard drive. The court would also order that the "mirror image" created by the expert be given to the defendant's counsel, who would retain custody of it throughout the litigation; defendant's counsel would then print and review any recovered documents and produce to the plaintiff any such documents that are responsive to discovery requests, creating a privilege log of any documents that are withheld on a claim of privilege [*Playboy Enters. v. Welles* (SD Cal 1999) 60 F Supp 2d 1050, 1054-1055 ; see *Visa Int'l Serv. Assoc. v. JSL Corp.* (D Nev Oct. 20, 2006) 2006 US Dist LEXIS 77451, at *12-*13 (adopting similar protocol for expert to create "image" of defendant's hard drive and recover deleted information); *Simon Prop. Group L.P. v. MySimon, Inc.* (SD Ind 2000) 194 FRD 639, 641-642 (adopting similar protocol for expert to recover deleted information from "mirror image" of hard drives of party's computers); see also *Experian Info. Solutions, Inc. v. I-Centrix, L.L.C.* (ND Ill July 21, 2005) 2005 US Dist LEXIS 42868, at *4-*10 (adopting similar protocol for expert to prepare "bitstream" of defendants' computers and to recover not only documents but also to evaluate "relevant contextual data" and "metadata" that would reveal information such as historical use of defendants' computers)].

Example:

In a copyright infringement action in federal court, the court found that the defendants might have had relevant information, in the form of stored or deleted computer files, programs, or e-mails, that was being overwritten by new data through the normal use of the computer equipment. The court also found, on the basis of an expert's affidavit, that such overwritten data could be recovered from the computer's hard drive. Accordingly, the court entered an order directing that the plaintiff's expert be given access to the defendants' computer equipment, for the purpose of copying and producing a "mirror image" of the

defendants' computer equipment (including any deleted information that the expert could recover). The order further required that the expert create two copies of the resulting data, to be provided to the court and to the defendants, but not to the plaintiff. Thereafter, whenever the plaintiff propounded a request for the production of documents, the defendants would sift through the data provided by the expert to locate and produce any relevant documents. Any disputed claim of privilege would be decided by the court through an in-camera review of the "mirror image" copy provided by the expert to the court [*Antioch Co. v. Scrapbook Borders, Inc.* (D Minn 2002) 210 FRD 645, 652-654] .



Cross Reference:

Court's power to appoint expert to copy electronic evidence, see 7.07[3][b].

7.07[2][d] Party Seeking Injunction May Argue Inadequacy of Legal Remedies for Spoliation of Evidence. In seeking to establish irreparable harm justifying issuance of an order preserving evidence, counsel may argue that the remedies for spoliation of evidence are often inapplicable or will not provide relief. The Civil Discovery Act [CCP § 2016.010 *et seq.*] does not provide an adequate remedy for the spoliation of electronic or other evidence. The Act's provisions for the use of "technology" in discovery do not address the question of remedies for spoliation of evidence [see CCP § 2017.710 *et seq.*]. Although the Act authorizes the court to issue protective orders to restrict discovery [see CCP §§ 2019.030, 2031.060], it does not provide a mechanism for the preservation of evidence or authorize the court to act on behalf of the party seeking evidence [*Dodge, Warren & Peters Ins. Servs., Inc. v. Riley* (2003) 105 CA4th 1414, 1419, 130 CR2d 385 ; *Northpoint Homeowners Assn. v. Superior Court* (1979); 95 CA3d 241, 243246, 157 CR 42] . Moreover, there is no tort of spoliation of evidence for either parties or third parties in California [see, e.g., *Coprich v. Superior Court* (2000) 80 CA 4th 1081, 1089-1090, 95 CR2d 884 ; *Cedars-Sinai Medical Center v. Superior Court* (1998) 18 C4th 1, 74 CR2d 248 , 954 P2d 1; *Temple Cmty. Hosp. v. Superior Court* (1999) 20 C4th 464, 476-478, 84 CR2d 852, 976 P2d 223] .

The availability of sanctions for misuse of discovery [see CCP § 2023.010 *et seq.*] may not establish an adequate remedy at law for the loss or destruction of evidence that is important to a party's case, because irreparable harm is likely to result when such evidence is destroyed [see *Dodge, Warren & Peters Ins. Servs., Inc. v. Riley* (2003) 105 CA4th 1414, 1419-1420, 130 CR2d 385 ; see also *Cedars-Sinai Med. Ctr. v. Superior Court* (1998) 18 C4th 1, 13-14, 74 CR2d 248, 954 P2d 511] .

Distinguish--Intentional Destruction and Innocent Loss of Electronically Stored Information:

Sanctions may be imposed for misuse of discovery, which generally includes intentional destruction of evidence in response to, or in anticipation of, a discovery request after litigation has commenced [*Cedars-Sinai Med. Ctr. v. Superior Court* (1998) 18 C4th 1, 12, 74 CR2d 248, 954 P2d 511 ; see CCP § 2023.010(d), (f)]. However, absent exceptional circumstances, the court has no power to impose sanctions on a party or any attorney for a party for a failure to provide discovery of electronically stored information that has been lost, damaged, altered, or overwritten as a result of the routine, good-faith operation of an electronic information system [CCP §§ 2031.060(i)(1), 2031.300(d)(1), 2031.310(j)(1), 2031.320(d)(1)].

Drawback--Obtaining Sanctions:

Possible sanctions for misuse of discovery include "issue sanctions" (ordering that designated facts be taken as established or precluding the offending party from supporting or opposing specified claims or defenses [CCP § 2023.030(b)]), "evidence sanctions" (prohibiting the offending party from introducing designated matters into evidence [CCP § 2023.030(c); see, e.g., *AdvantaCare Health Partners, LP v. Access IV* (ND Cal Aug. 17, 2004) 2004 U.S. Dist. LEXIS 16835, at *21-*23 (defendants' deletion of their computer files in violation of temporary restraining order warranted imposition of evidence sanction consisting of presumption that defendants had copied every file on plaintiff's computer system)]), and "terminating sanctions" (such as striking part or all of the pleadings, dismissing part or all

of the action, or granting a default judgment against the offending party [CCP § 2023.030(d); see, e.g., *Columbia Pictures, Inc. v. Bunnell* (CD Cal Dec. 13, 2007) 2007 US Dist LEXIS 96360, at *15-*25 (imposing termination sanction for defendants' willful spoliation of evidence that inalterably prejudiced plaintiffs' ability to prove their case); *R.S. Creative, Inc. v. Creative Cotton, Ltd.* (1999) 75 CA4th 486, 496-498, 89 CR2d 353 (affirming imposition of terminating sanction for repeated violations of stipulations and court orders, including deliberate destruction of electronic evidence pertinent to exposing forgery of contract underlying complaint))].

Although these sanctions theoretically would be available after the destruction of electronic evidence, a court may be reluctant to impose them without a showing that the destroyed evidence was indispensable or that the destruction of evidence was motivated by bad faith [see, e.g., *Creative Sci. Sys. v. Forex Capital Mkts., LLC* (ND Cal Apr. 4, 2006) 2006 U.S. Dist. LEXIS 20116, at *17-*22 (imposing monetary sanctions, but not issue or evidence sanctions, because record did not contain convincing evidence that bad faith had motivated party's reinstallation of computer operating systems, which resulted in loss of relevant data)]. That showing may be difficult or impossible to make if the electronic evidence has been destroyed and its precise contents lost, or if the record is inconclusive about the reasons for the loss of evidence. On this basis, it may be argued that despite the theoretical availability of issue sanctions, evidence sanctions, and terminating sanctions, the actual imposition of those sanctions is not assured, making them an inadequate potential remedy for a loss or destruction of electronically stored information that is likely to be sought in discovery.

Cross Reference:

Sanctions for misuse of discovery, including spoliation of evidence, see *Ch. 13, Seeking or Opposing Sanctions for Noncompliance*, 13.03-13.10.

7.07[3] Court May Issue Injunction Tailored to Circumstances of Case.

7.07[3][a] Court May Issue Nonspoliation Order. In exercising its authority to issue an injunctive order for the preservation of electronically stored information pending discovery, the court may expressly require a party to maintain and store the relevant information, and prohibit that party from destroying, deleting, or secreting from discovery any of the information [see *Dodge, Warren & Peters Ins. Servs., Inc. v. Riley* (2003) 105 CA4th 1414, 1417, 130 CR2d 385 ; see also *Pueblo of Laguna v. United States* (2004) 60 Fed Cl 133, 141-143 (ordering defendant to preserve specified evidence, index all evidence reasonably anticipated to be subject to discovery, and report immediately any loss or destruction of records)].

Example:

An insurance brokerage firm sued its former employees, claiming misappropriation of trade secrets, unfair business practices, breach of fiduciary duty, and breach of contract. The plaintiff sought a preliminary injunction to preserve electronically stored information copied by the defendants from the plaintiff's computers. The court of appeal affirmed the trial court's grant of an injunction that included, among other terms, a provision expressly prohibiting the defendants from destroying, deleting, or secreting from discovery any of their electronic storage media [*Dodge, Warren & Peters Ins. Servs., Inc. v. Riley* (2003) 105 CA4th 1414, 1417, 130 CR2d 385] .

7.07[3][b] Court May Issue Order Requiring Neutral Expert to Seize and Copy Electronic Evidence. In exercising its authority to issue an injunctive order for the preservation of electronically stored information pending discovery, the court may appoint or require the parties to appoint an expert to carry out the process of seizing, copying, recovering, and storing the relevant information [see *Dodge, Warren & Peters Ins. Servs., Inc. v. Riley* (2003) 105 CA4th 1414, 1417, 130 CR2d 385] .

Example:

An insurance brokerage firm sued its former employees, claiming misappropriation of trade secrets, unfair business practices, breach of fiduciary duty, and breach of contract. The plaintiff sought a preliminary injunction to preserve electronically stored information copied by the defendants from the plaintiff's computers. The court of appeal affirmed the trial court's grant of an injunction that required, among other things, that the defendants allow a court-appointed expert (1) to copy all of their electronic storage media, including computer hard drives and discs; (2) to recover lost or deleted files; (2) and to perform automated searches of that evidence under guidelines agreed to by the parties or established by the court [*Dodge, Warren & Peters Ins. Servs., Inc. v. Riley* (2003) 105 CA4th 1414, 1417, 130 CR2d 385] .

Example:

In a trademark infringement action in federal court, the court found it likely that relevant information was stored on the hard drive of the defendant's computer, in the form of deleted e-mails. After finding that the plaintiff's need for the information outweighed the burden on the defendant of allowing access to her computer, the court ordered that the plaintiff provide evidence that recovering some of the deleted e-mails was at least as likely as not recovering any of the e-mails, and that no damage would be done to the defendant's computer in the recovery process. If such evidence could be provided, the court stated that it would make the following orders: (1) the court would appoint a computer expert to create a "mirror image" of the defendant's hard drive; (2) the expert would serve as an officer of the court, so that allowing the expert access to the hard drive would not constitute a waiver by the defendant of attorney-client privilege as to any information on the hard drive; (3) the "mirror image" created by the expert would be given to the defendant's counsel, who would retain custody of it throughout the litigation; and (4) the defendant's counsel would print and review any recovered documents and produce to the plaintiff any such documents that are responsive to discovery requests, creating a privilege log of any documents that are withheld on a claim of privilege [*Playboy Enters. v. Welles* (SD Cal 1999) 60 F Supp 2d 1050, 1054-1055 ; see *Visa Int'l Serv. Assoc. v. JSL Corp.* (D Nev Oct. 20, 2006) 2006 US Dist LEXIS 77451, at *12-*13 (adopting similar protocol for expert to create "image" of defendant's hard drive and recover deleted information); *Antioch Co. v. Scrapbook Borders, Inc.* (D Minn 2002) 210 FRD 645, 652-654 (adopting similar protocol in copyright infringement action for expert to create "mirror image" of defendants' computer equipment); *Simon Prop. Group L.P. v. MySimon, Inc.* (SD Ind 2000) 194 FRD 639, 641-642 (adopting similar protocol for expert to recover deleted information from "mirror image" of hard drives of party's computers); see also *Experian Info. Solutions, Inc. v. I-Centrix, L.L.C.* (ND Ill July 21, 2005) 2005 US Dist LEXIS 42868, at *4-*10 (adopting similar protocol for expert to prepare "bitstream" of defendants' computers and to recover not only documents but also to evaluate "relevant contextual data" and "metadata" that would reveal information such as historical use of defendants' computers)].



83 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery

II. PLANNING FOR PRESERVATION OF ELECTRONIC EVIDENCE

1-7 MB Practice Guide: CA E-Discovery and Evidence 7.08

7.08 Weighing Advantages and Disadvantages of Seeking Order to Preserve Electronic Evidence.

7.08[1] Advantages and Disadvantages of Seeking Injunctive Order.

7.08[1][a] Ex Parte Order May Be Obtained on Short or No Notice on Showing of Great or Irreparable Injury. An ex parte temporary restraining order may be obtained on shortened notice or no notice at all [*CCP* § 527(c)]. This can be a great advantage, particularly if counsel suspects that the adverse party might intentionally destroy damaging evidence.

However, the threshold requirement to obtain an order ex parte (for example, that great or irreparable injury will result before a noticed motion can be heard [*see CCP* § 527(c)(1)]) may be difficult to meet, particularly if there is no indication that evidence will be destroyed intentionally.

Cross Reference:

Ex Parte Application Procedures, *see* 7.11.

7.08[1][b] If Showing Required for Ex Parte Order Cannot Be Made, Time and Cost Factors May Make Noticed Motion for Injunction Undesirable. If the threshold showing for an ex parte order cannot be made, then the time required to make a noticed motion for a preliminary injunction and obtain a ruling [*see CCP* § 1005(b) (notice of motion generally must be served at least 16 court days before hearing)] will not be appreciably shorter than the time needed to obtain a response to a request for production of the electronic evidence itself [*see CCP* § 2031.030(c)(2) (demand for inspection or copying of electronically stored information generally must allow at least 30 calendar days for production)]. In addition, the expense of pursuing a noticed motion will surely exceed the cost involved in making a standard discovery request.

Cross Reference:

Procedure for noticed motion, *see* 7.12.

7.08[1][c] Applicant Must Provide Bond or Undertaking. Whenever a court issues a preliminary injunctive order, it must require an undertaking by the applicant or movant, to indemnify the responding party for any damage that party might suffer if it is ultimately determined that the injunction should not have been granted [*CCP* § 529(a)]. This

requirement applies when the court issues a preliminary injunction to preserve evidence [*Northpoint Homeowners Assn. v. Superior Court* (1979) 95 CA3d 241, 246, 157 CR 42] .

7.08[2] Alternative Approaches Should Be Considered. As an alternative to seeking an injunction to preserve electronic evidence, counsel may consider the following alternative approaches:

- Seeking an order for expedited discovery, including shortening the regular timetable for discovery of electronically stored information [see CCP §§ 2031.020(b), (d), 2031.030(c)(2); see, e.g., *Physicians Interactive v. Lathian Sys. Inc.* (ED Va Dec. 5, 2003) 2003 US Dist LEXIS 22868, at *29-*30 (granting limited expedited discovery to obtain "mirror image" of relevant information on defendants' computer equipment)].

➡ **Cross References:**

Expedited discovery, see 7.10[2].

Motion to shorten discovery timetable, see *Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 10, Making Demands for Inspection, 10.04.*

- Sending the adverse party written notice that the discovery of electronically stored information is reasonable likely to be sought, and then meeting and conferring with opposing counsel to arrive at an agreement regarding the preservation and discovery of that information [see *Cal Rules Ct, Rule 3.724(8)*].

➡ **Cross Reference:**

Notice that discovery of electronically stored information is reasonably likely to be sought, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferring, and Case Management Conference, 5.09-5.13.*

- Raising issues pertaining to the preservation and discovery of electronically stored information at the case management conference [see *Cal Rules Ct, Rule 3.278(13),(14)*; see also *Cal Rules Ct, Rule 3.274(b)(1)*].

➡ **Cross Reference:**

Discussion of case management conference, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferring, and Case Management Conference, 5.22-5.25.*

- Relying on the deterrent effect of other provisions and sanctions available under California law, which include [*Temple Cmty. Hosp. v. Superior Court* (1999) 20 C4th 464, 476-477, 84 CR2d 852, 976 P2d 223] :

- ☐ Discovery sanctions to punish third party spoliation, including monetary and contempt sanctions against persons who flout the discovery process by suppressing or destroying evidence [see CCP §§ 2020(h), 2023(b)(1), (5), 2025(j)(3)(o); *Brun v. Bailey* (1994) 27 CA4th 641, 658-659, 32 CR2d 624 (reference to "any person" in statute imposing discovery sanctions permits sanctions against nonparty)].

- ☐ Criminal sanctions under *Pen Code § 135.*

- ☐ Disciplinary sanctions against attorneys who may be involved in spoliation.
- ☐ Demonstrating at trial why the spoliated evidence is missing [*Evid Code* § 412].
- ☐ Establishing a connection between the spoliator and a party to the litigation sufficient to invoke the sanctions applicable to spoliation by a party [*CCP* § 2025(j)(3), (o)].



Cross Reference:

Discussion of sanctions, Ch. 13, Seeking or Opposing Sanctions for Noncompliance.



84 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery

III. OBTAINING INJUNCTION TO PRESERVE ELECTRONIC EVIDENCE

1-7 MB Practice Guide: CA E-Discovery and Evidence 7.09

7.09 CHECKLIST: Obtaining Injunction To Preserve Electronic Evidence.

- ☐ Determine whether to seek injunction by ex parte application.

Authority:

CCP § 527(c); Cal Rules Ct, Rule 3.1202(c)

Discussion:

See 7.10[1], 7.11

☐ Consider whether opposing party is likely to attempt to delete or destroy damaging electronic evidence, and whether party requesting ex parte injunction can make adequate showing to that effect.

☐ Consider whether use of regular noticed motion would result in irreparable harm; for example, by allowing opposing party time to destroy electronic evidence that is essential to movant's case.

- ☐ If proceeding ex parte, prepare necessary documents.

☐ Prepare ex parte application for temporary restraining order.

Authority:

CCP § 527(c); Cal Rules Ct, Rules 3.1201(1), 3.1202(a)

Form:

See 7.16

☐ Include name, address, and telephone number of attorney for any party (or if no such attorney is known, name, address, and telephone number of party).

☐ Identify electronic information sought to be protected.

☐ Specify acts to be prohibited.

☐ If desired, request that court order seizure and copying of electronic evidence by independent expert.

☐ If advance notice of application will not be given to opposing party, include request for order to show cause why court should not issue preliminary injunction continuing protection provided by temporary restraining order.

Authority:

CCP § 527(c)(2)(C), (d)(1); Cal Rules Ct, Rule 3.1204(b)(3)

☐ Prepare affidavits or declarations to establish that great or irreparable injury will result to applicant before matter can be heard on notice.

Authority:

CCP § 527(c)(1); Cal Rules Ct, Rules 3.1201(2), 3.1202(a)

Form:

See 7.17

☐ Prepare declaration of applicant's counsel, certifying one of following:

Authority:

CCP § 527(c)(2); Cal Rules Ct, Rules 3.1201(3), 3.1204(b)

Form:

See 7.17

☐ Within reasonable time before application is made, applicant or applicant's counsel informed opposing party or opposing party's counsel at what time and where application would be made.

☐ Applicant or applicant's counsel in good faith attempted but was unable to inform opposing party or opposing party's counsel the application would be made.

☐ For reasons specified in statement, applicant should not be required to provide opposing party or opposing party's counsel advance notice of application.

- ☐ Prepare memorandum in support of application.

Authority:

Cal Rules Ct, Rule 3.1201(4)

- ☐ Prepare proposed order to show cause and temporary restraining order.

Authority:

Cal Rules Ct, Rules 3.1150(c), 3.1201(5)

Form:

See 7.19

- ☐ If proceeding ex parte, unless counsel has reason not to provide opposing party advance notice of application, serve copies of application and accompanying documents at reasonable time, usually no later than 10 a.m. on court day before ex parte appearance.

Authority:

CCP § 527(c)(2)(A), (C); Cal Rules Ct, Rule 3.1203(a)

- ☐ If proceeding ex parte, file application and accompanying documents, and appear personally in court to present application.

Authority:

Cal Rules Ct, Rules 3.1205, 3.1207

- ☐ If proceeding by noticed motion, prepare necessary documents.

- ☐ Prepare notice of motion and motion for preliminary injunction, including specification of one or both of following grounds for motion:

Authority:

CCP § 526(a); Cal Rules Ct, Rules 3.1110, 3.1112(a)

Discussion:

See 7.12[1][a]

Form:

See 7.20

- ☐ Loss or destruction of electronic evidence described in motion would cause great or irreparable harm to movant, by depriving movant of relevant evidence.

Authority:

CCP § 526(a)(2)

☐ It appears that opposing party, by causing or allowing destruction of electronic evidence, is or would be acting in violation of movant's rights, effectively rendering any judgment ineffectual.

Authority:

CCP § 526(a)(3); Dodge, Warren & Peters Ins. Servs., Inc. v. Riley (2003) 105 CA4th 1414, 1418-1419, 130 CR2d 385

☐ Prepare memorandum in support of motion.

Authority:

Cal Rules Ct, Rule 3.1112(a)(3)

☐ Prepare affidavits or declarations, along with any appropriate exhibits, that are necessary to provide factual support for motion.

Authority:

Cal Rules Ct, Rule 3.1112(b)

☐ If proceeding by noticed motion, follow standard motion procedure.

Authority:

Cal Rules Ct, Rule 3.1300 et seq.



Cross Reference:

See 7.12



85 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery
 III. OBTAINING INJUNCTION TO PRESERVE ELECTRONIC EVIDENCE

1-7 MB Practice Guide: CA E-Discovery and Evidence 7.10

7.10 Options and Strategies.

7.10[1] Decide Whether to Proceed Ex Parte. If counsel has reason to believe that the opposing party is likely to attempt to delete or destroy damaging electronic evidence before the court can issue an injunction to preserve the evidence, the motion should proceed ex parte.

Prerequisites:

Generally, an ex parte application must be supported by an affirmative factual showing of irreparable harm, immediate danger, or any other statutory basis for granting ex parte relief [*Cal Rules Ct, Rule 3.1202(c)*]. In determining whether to proceed ex parte in seeking an injunction to preserve electronic evidence, therefore, counsel should assess whether the circumstances indicate that the evidence sought is likely to be destroyed, modified, or concealed if notice of the lawsuit is given.

**Strategic Point--Moving Party:**

The court has the option of treating an ex parte application as a motion for a preliminary injunction; if the court chooses this option, the matter will proceed as a regular noticed motion [*see Dodge, Warren & Peters Ins. Servs., Inc. v. Riley (2003) 105 CA4th 1414, 1418-1419, 130 CR2d 385*].

**Cross Reference:**

Discussion of noticed motion for preliminary injunction to preserve electronic evidence, see 7.12.

7.10[2] Decide What Terms to Request in Injunctive Order. Depending on the circumstances, such as the format or media in which the electronic evidence is stored, the potential disruption of the adverse party's business operations that might result from each of the following orders, and any known facts indicating that the adverse party might be tempted to tamper with evidence subject to an injunctive order, counsel should consider whether to seek one or more of the following orders:

**Cross References:**

Forms, see 7.22, 7.23.

- A nonspoliation order, prohibiting the adverse party from deleting, destroying, or tampering with specified electronically stored information in the form in which it exists as of a specific date, during the pendency of the suit or until further order of the court.
- An order requiring the adverse party to make a copy of specified electronic evidence, using a specified storage medium, and to retain the copy during the pendency of the suit or until further order of the court.
- An order appointing an independent expert to seize specified electronic evidence and make a copy for use in discovery. Such an order may include a requirement that the expert review and screen the electronic evidence for privileged materials or other materials specific by the court.
- An order providing for expedited discovery, which is often sought in conjunction with these remedies.



Strategic Point--Expedited Discovery:

Ordinarily a plaintiff must wait until 10 days after the service of the summons or appearance of the other party, whichever occurs first, to make a demand for inspection of electronically stored evidence without leave of court [CCP § 2031.020(a)]. Furthermore, a plaintiff making such a demand ordinarily must specify a reasonable time for inspection that is at least 30 days after the service [CCP § 2031.030(c)(2)]. However, on motion with or without notice, the court, for good cause shown, may grant the plaintiff leave to make an inspection demand at an earlier time [CCP § 2031.020(b)], and/or grant the plaintiff leave to specify an earlier inspection date [CCP § 2031.030(c)(2)]. Although the 10-day and 30-day periods may have little or no impact in most cases, they may be a source of concern if the plaintiff is concerned that the delay may result in loss or destruction of the electronically stored evidence, either through intentional destruction, inadvertence, or the operation of normal corporate data management procedures. When that is the case, an order authorizing immediate discovery may be requested in connection with the injunction.

Example:

In a copyright infringement action in federal court, in which the defendants appeared pro se, the plaintiff asserted that the defendants had stated they would be going out of business, which caused the plaintiff concern that the defendants' electronic business records might be lost or destroyed. The defendants also had previously refused to allow the plaintiff's computer expert to copy the hard drives of the defendants' computers. The plaintiff expressed a belief that the defendants, one of whom was a former employee of the plaintiff, harbored resentment toward the plaintiff that could result in the defendants' destruction of relevant computer records. The plaintiff also believed that the defendants, lacking legal representation, might not fully appreciate the nature of the discovery process. Taking these circumstances into account, the court granted (1) the plaintiff's unopposed motion for an order directing the parties to preserve all relevant documents, (2) the plaintiff's motion to expedite discovery, and (3) the plaintiff's motion to appoint a neutral expert to recover information that had been deleted from the defendants' computers [*Antioch Co. v. Scrapbook Borders, Inc.* (D Minn 2002) 210 FRD 645, 649-654] .



86 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery
III. OBTAINING INJUNCTION TO PRESERVE ELECTRONIC EVIDENCE

1-7 MB Practice Guide: CA E-Discovery and Evidence 7.11

7.11 Making Ex Parte Application for Temporary Restraining Order to Preserve Electronic Evidence.

7.11[1] Party Seeking Order Must Prepare Moving Papers.

7.11[1][a] Party Seeking Order Must Prepare Ex Parte Application. An ex parte application for a temporary restraining order to preserve electronic evidence must be in writing [*Cal Rules Ct, Rule 3.1201*] and must include the following:

- The case caption [*Cal Rules Ct, Rule 3.1201(1)*].
- A statement of the injunctive relief requested [*Cal Rules Ct, Rule 3.1201(1)*]. This statement should include a specific description of the evidence sought to be preserved and, if known, the medium in which it is stored.



Warning--Scope of Requested Order Should Not Be So Broad As to Be Unworkable.

A blanket preservation order runs the risk of being unworkable. Computers automatically delete, create, and overwrite information in the course of normal operations. A blanket order that would effectively result in cessation of all of a party's computer operations could effectively paralyze the party's activities, as well as being prohibitively expensive, and therefore is likely to be more difficult to obtain. As a general matter, the preservation of discoverable evidence should be discussed by the parties early in the litigation [see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference, 5.14-5.21*].

- A request for an order to show cause why a preliminary injunction should not issue [*Cal Rules Ct, Rule 3.1150(a)*].
- The name, address, and telephone number of any attorney known to the applicant to be an attorney for any party or, if no attorney is known for a party, the name, address, and telephone number of the party if known to the applicant [*Cal Rules Ct, Rule 3.1202(a)*].

● If an ex parte application for an order to preserve evidence has been made to the court and refused in whole or in part, the current application, even if made on an alleged different state of facts, must include a full disclosure of any previous applications and the court's actions on the previous applications [*Cal Rules Ct, Rule 3.1202(b)*].

7.11[1][b] Application Must Be Accompanied by Declarations Establishing Basis for Ex Parte Relief. An ex parte application for a temporary restraining order to preserve electronic evidence must be accompanied by one or more declarations, containing competent testimony based on personal knowledge, that make a factual showing that great or irreparable harm will result to the applicant before the matter can be heard on notice [*CCP § 527(c)(1); Cal Rules Ct, Rules 3.1201(2), 3.1202(c)*]. Thus, for example, the facts established by the declarations should indicate that the evidence sought is likely to be destroyed, modified, or concealed if notice of the lawsuit or notice of a motion for a preliminary injunction is given.



Strategic Point:

Evidence that the party from whom discovery will be sought has destroyed or concealed evidence before the lawsuit is the most often used basis for issuance of an ex parte preservation order [*see Ophir D. Finkelthal, Scope of Electronic Discovery and Methods of Production, 38 Loy. L.A. L. Rev. 1591, 1600-1601 (2005); see, e.g., AdvantaCare Health Partners, LP v. Access IV (ND Cal Aug. 17, 2004) 2004 U.S. Dist. LEXIS 16835, at *4 (plaintiffs obtained temporary restraining order after learning that defendant had deleted evidence that he had copied plaintiffs' confidential and proprietary information)*]. Such evidence must consist of a showing, for example, of specific instances in which the party from whom discovery will be sought (or a person connected to the party) has destroyed evidence or willfully violated court orders in the past [*see Adobe Sys., Inc. v. South Sun Prods., Inc. (SD Cal 1999) 187 FRD 636, 641 (citing First Tech. Safety Sys., Inc. v. Depinet (6th Cir. 1993) 11 F3d 641, 651)*]. In the absence of such evidence, however, a general assertion that electronic evidence can easily be deleted or destroyed will be insufficient to justify ex parte injunctive relief [*Adobe Sys., Inc. v. South Sun Prods., Inc. (SD Cal 1999) 187 FRD 636, 640*].

Distinguish:

The showing of irreparable harm justifying ex parte relief is different from the showing of irreparable injury necessary to support injunctive relief. The former focuses on whether irreparable harm is likely to result from giving the adverse party notice that the lawsuit or application for injunctive relief is pending [*see CCP § 527(c)(1); Cal Rules Ct, Rule 3.1202(c)*], while the latter focuses on the harm that would arise from the loss of the evidence sought to be preserved [*see CCP § 527(a)*]. For example, if relevant evidence is in danger of inadvertent destruction through the routine, good-faith operation of a party's computer system, notice of the lawsuit ordinarily would not increase the risk of destruction of the evidence (in fact, it might decrease the risk of loss by making the party aware of the importance of the evidence). In such a case, the harm that would result from the loss of the evidence might justify injunctive relief, but it does not justify granting such relief ex parte. On the other hand, if notice of the lawsuit is likely to increase the risk of intentional destruction of the evidence, then a grant of ex parte relief may be justified.



Cross Reference:

Discussion of declarations establishing statutory grounds for injunctive relief, *see 7.11[1][c]*.

7.11[1][c] Application Must Be Accompanied by Declarations Establishing Basis for Injunction. An ex parte application for a temporary restraining order to preserve electronic evidence must be accompanied by one or more declarations, containing competent testimony based on personal knowledge, that establish facts sufficient to support a finding of the existence of one or more grounds for injunctive relief [*see CCP § 526(a)*], such as the following:

- The loss or destruction of the evidence sought to be preserved would cause great or irreparable injury to the applicant, by depriving him or her of the ability to present relevant evidence that is necessary to establish a claim or defense in the litigation [CCP § 526(a)(2)].

- The adverse party is doing, is threatening, is about to do, or is procuring or allowing to be done some act in violation of the applicant's rights that would result in the loss or destruction of relevant evidence, thus rendering an eventual discovery request by the applicant ineffectual [CCP § 526(a)(3); see *Dodge, Warren & Peters Ins. Servs., Inc. v. Riley* (2003) 105 CA4th 1414, 1418-1419, 130 CR2d 385] .

- The evidence sought to be preserved is critical to the applicant's ability to prove his or her claim or defense, and the monetary value of the claim or defense would be extremely difficult to calculate, such that pecuniary compensation for the loss or destruction of the evidence would not afford adequate relief [CCP § 526(a)(4), (5)].

- The issuance of the requested injunctive relief would result in only minor harm to or burden for the opposing party, for example, because it would not interrupt the opposing party's ability to conduct its business operations or cause the disclosure of the opposing party's trade secrets or other confidential and proprietary business information [see *Dodge, Warren & Peters Ins. Servs., Inc. v. Riley* (2003) 105 CA4th 1414, 1421, 130 CR2d 385 ; see also CCP § 2017.020(a)].

7.11[1][d] Application Must Be Accompanied by Declaration of Notice. An ex parte application for a temporary restraining order to preserve electronic evidence must be accompanied by a declaration regarding notice, stating one of the following [Cal Rules Ct, Rules 3.1201(3), 3.1204(b)]:

- For each party notified of the application, the name of the person informed; the date, time, manner of giving notice; the relief sought; any response; whether opposition is expected; and that the applicant informed the opposing party, by 10 a.m. the court day before the ex parte appearance, where and when the application would be made [see Cal Rules Ct, Rule 3.1203(a)]. If notice was provided later than that time, the declaration must explain the exceptional circumstances that justify the shorter time for notice [Cal Rules Ct, Rule 3.1203(a), 3.1204(c)(1)].

- That the applicant in good faith attempted to inform each opposing parties but was unable to do so, specifying the efforts made to inform the opposing party.

- The reasons why the applicant should not be required to inform an opposing party.

Cross Reference:

Form, see 7.17.

7.11[1][e] Application Must Be Accompanied by Supporting Memorandum. An ex parte application for a temporary restraining order to preserve electronic evidence must be accompanied by a supporting memorandum [Cal Rules Ct, Rules 3.1201(4), 3.1113]. The memorandum should include arguments showing that the facts set forth in the supporting declarations establish the existence of one or more grounds for injunctive relief [Cal Rules Ct, Rule 3.1113(b); see CCP § 526(a)].

Cross Reference:

Declarations setting forth facts constituting grounds for injunctive relief, see 7.18.



Warning:

The court may construe the absence of a supporting memorandum as an admission that the motion is not meritorious, and deny the motion [*Cal Rules Ct, Rule 3.1113(a)*].

7.11[1][f] Application Must Be Accompanied by Proposed Order. An ex parte application for a temporary restraining order to preserve electronic evidence must be accompanied by a proposed order [*Cal Rules Ct, Rule 3.1201(5)*]. The proposed order must state an order to show cause (OSC) why a preliminary injunction should not issue; when the order is served, the OSC will be the equivalent of a notice of motion for a preliminary injunction [*Cal Rules Ct, Rule 3.1150(a), (c)*].

After the OSC, the order must separately state a temporary restraining order describing the activities that are enjoined pending the hearing on the preliminary injunction [*Cal Rules Ct, Rule 3.1150(c)*].

The proposed OSC must contain blank spaces for the time and manner of service on responding parties, the date on which proof of service must be delivered to the court, a briefing schedule, and, if applicable, the expiration date of the temporary restraining order [*Cal Rules Ct, Rule 3.1150(c)*].

The proposed order must be lodged and served with, but not attached to, the moving papers [*Cal Rules Ct, Rule 3.1113(m)*].

7.11[2] Applicant Must Serve Notice of Ex Parte Application. The applicant generally must notify all parties of the ex parte application, stating with specificity the nature of the relief to be requested and the date, time, and place for the presentation of the application [*Cal Rules Ct, Rule 3.1204(a)(1)*]. The applicant must also attempt to determine whether any opposing party will appear to oppose the application [*Cal Rules Ct, Rule 3.1204(a)(2)*].

In addition, the applicant, at the first reasonable opportunity, must serve the ex parte application on all other parties that will appear at the ex parte hearing. Absent exceptional circumstances, no hearing may be conducted unless service has been made [*Cal Rules Ct, Rule 3.1206*].



Timing:

The notice of an ex parte application generally must be given to all parties not later than 10 a.m. the court day before the ex parte appearance. Exceptions exist if there are reasons not to notify the opposing party or if exceptional circumstances justify a shorter time for notice. A declaration accompanying the ex parte application will need to state the reasons why notice should not be required or the exceptional circumstances justifying shorter notice [*Cal Rules Ct, Rule 3.1203(a), 3.1204(c)*].



Cross Reference:

Discussion of declaration regarding notice, see 7.11[1][d].

7.11[3] Ex Parte Application Should Be Presented to Court. The ex parte application should be presented to the superior court judge or commissioner to whom the case has been assigned; if the case has not been assigned, the application should be presented to the presiding judge of the court or to the law and motion judge, depending on local practice [see *CCP § 166(a)(1), CCP § 259(a)*].

If the complaint was filed earlier that same day, the applicant also must provide a file-stamped copy of the complaint to the judge who will hear the ex parte application [*Cal Rules Ct, Rule 3.1150(b)*]. Otherwise, if a court file has already been established, the applicant must request that the court file be made available to the judge hearing the ex parte application [*Cal Rules Ct, Rule 3.1150(b)*].

7.11[4] Applicant Must Appear Before Court Unless Parties Have Stipulated to Order. The court will not consider an ex parte application for a temporary restraining order to preserve electronic evidence unless the applicant or

applicant's counsel personally appears or unless the parties have stipulated to the order [*Cal Rules Ct, Rule 3.1207*].



Strategic Point:

Once a TRO application has been made, it is not uncommon for the parties to meet and confer before or at the court hearing and enter into a stipulated TRO preserving evidence and allowing expedited discovery, with or without court involvement and approval.

7.11[5] Order Must Be Signed, Filed, and Served. If the ex parte application is granted, the judge or commissioner will sign the original of the order. Counsel then should have the copies conformed by the courtroom clerk or by a deputy clerk in the court clerk's office and have the originals of the application and the order filed if they have not already been taken by the courtroom clerk for filing.

Counsel must serve a conformed copy of the order, together with a copy of the written ex parte application, on opposing counsel or on the opposing party if not represented by counsel [*see CCP § 1015*].

Unless the court orders otherwise, notice of the order to show cause and temporary restraining order must be given by the applicant to all other parties or their attorneys, unless notice is waived by all parties in open court and is entered in the minutes [*CCP § 1019.5(a)*].



87 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery

III. OBTAINING INJUNCTION TO PRESERVE ELECTRONIC EVIDENCE

*1-7 MB Practice Guide: CA E-Discovery and Evidence 7.12***7.12 Making Noticed Motion for Preliminary Injunction to Preserve Electronic Evidence.****7.12[1] Party Seeking Order Must Prepare Moving Papers.**

7.12[1][a] Party Seeking Order Must Prepare Notice of Motion and Motion. The papers that must be filed in support of a motion for a preliminary injunction to preserve electronic evidence include a notice of hearing on the motion and the motion itself [*Cal Rules Ct, Rule 3.1112(a)*]. These papers, and any other papers filed in support of the motion, may be filed as separate documents or may be combined in one or more documents if the movant specifies each included item separately in the caption of the combined document [*Cal Rules Ct, Rule 3.1112(c)*].

The motion for a preliminary injunction must identify the party or parties bringing the motion, name the parties to whom it is addressed, and briefly state the basis for the motion and the relief sought [*Cal Rules Ct, Rule 3.1112(d)*].

The notice of motion must state in the opening paragraph the nature of the order being sought and the grounds for issuance of the order, and it must otherwise comply with the standard requirements for a notice of motion [*Cal Rules Ct, Rule 3.1110(a)*].

 Cross Reference:

Standard format for notice of motion, see *Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure, Ch. 26, 26.39-26.45*.

7.12[1][b] Motion Must Be Accompanied by Supporting Declarations. A motion should be accompanied one or more declarations that establish the factual grounds for the injunction sought. A declaration may include exhibits or appendices as appropriate, authenticated by the declarant [*see Cal Rules Ct, Rule 3.1112(b)*].

 Cross Reference:

Discussion of content of supporting declarations, see *7.11[1][c]*.

**Strategic Point:**

Although not required for a motion for a preliminary injunction to preserve electronic evidence, a

declaration that counsel met and conferred with opposing counsel (or offered to meet and confer) [see *Cal Rules Ct, Rule 3.724(8)*] in an unsuccessful attempt to resolve the issues presented by the motion might help convince the court of the need for injunctive relief [see *CCP § 2016.040*].

7.12[1][c] Motion Must Be Accompanied by Request for Judicial Notice If Notice Is Being Requested. A party requesting judicial notice of material relevant to the motion [see *Evid Code §§ 452, 453*] must provide the court and each party with a copy of the material. If the material is already part of the court's file, the party must [see *Cal Rules Ct, Rules 3.1113(l)>, 3.1306(c)*]:

- Specify in writing the part of the file sought to be judicially noticed; and
- Make arrangements with the clerk to have the file in the courtroom at the time of the hearing.

7.12[1][d] Party Seeking Permission to Present Oral Testimony Must File Written Statement. A party seeking permission to introduce oral evidence (except for oral evidence in rebuttal to oral evidence presented by the other party) must file, no later than three court days before the hearing, a written statement of the nature and extent of the evidence to be introduced and a reasonable time estimate for the hearing. If the statement is filed less than five court days before the hearing, the filing party must serve a copy on the other parties in a manner to assure delivery no later than two days before the hearing [see *Cal Rules Ct, Rule 3.1306(b)*].

7.12[1][e] Motion Must Be Accompanied by Supporting Memorandum. A motion for a preliminary injunction to preserve electronic evidence must be accompanied by a supporting memorandum [see *Cal Rules Ct, Rules 3.1112(a), 3.1113*]. The memorandum should include arguments showing that the facts set forth in the supporting declarations establish the existence of one or more grounds for injunctive relief [see *Cal Rules Ct, Rule 3.1113(b)*; see *CCP § 526(a)*].



Cross Reference:

Discussion of declarations setting forth facts constituting grounds for injunctive relief, see 7.11[1][c].



Warning:

The court may construe the absence of a supporting memorandum as an admission that the motion is not meritorious and therefore deny the motion [see *Cal Rules Ct, Rule 3.1113(a)*].

7.12[1][f] Motion Must Be Accompanied by Proposed Order. If the movant submits a proposed order, it must be lodged and served with, but not attached to, the moving papers [see *Cal Rules Ct, Rule 3.1113(m)*].

7.12[2] Moving Papers Must Be Filed in Clerk's Office.

Unless otherwise provided by local rule, the moving papers must be filed in the clerk's office [see *Cal Rules Ct, Rule 3.1302(a)*].



Timing:

The moving papers must be filed within the time provided for serving the motion, unless the court for good cause prescribes a shorter time [see *CCP § 1005(b)*; *Cal Rules Ct, Rule 3.1300(a), (b)*]. Papers submitted before the close of the clerk's office on the day the papers are due are deemed timely filed [see *Cal Rules Ct, Rule 3.1300(e)*]. No paper may be rejected for filing on the ground that it was untimely submitted. However, the court, in its discretion, may refuse to consider a late filed paper; in this situation, the minutes or order must so indicate [see *Cal Rules Ct, Rule 3.1300(d)*].



Cross Reference:

Time for serving moving papers, see 7.12[3].

7.12[3] Motion Must Be Served and Filed Within Applicable Time Limits. Unless otherwise ordered or specifically provided by law, copies of all moving and supporting papers ordinarily must be served and filed at least 16 court days before the hearing on the motion [*CCP § 1005(b)*; *Cal Rules Ct, Rule 3.1300(a)*]. Proof of service must be filed no later than five court days before the time appointed for the hearing [*Cal Rules Ct, Rules 2.250*].

Exceptions--Service by Means Other Than Personal Service:

- If the moving papers are served by regular mail, the 16-day period increases by five calendar days if the places of mailing and the mailing address are in California, by 10 calendar days if either the place of mailing or the mailing address is outside California but within the United States, and by 20 calendar days if either the place of mailing or the mailing address is outside the United States [*CCP § 1005(b)*].
- If the notice is served by express mail, or another method of overnight delivery, the 16-day period is increased by two calendar days [*CCP § 1005(b)*].
- If the notice is served by facsimile transmission pursuant to the parties' agreement, the 16-day period increases by two calendar days [*CCP § 1005(b)*; see *CCP § 1013(e)*; *Cal Rules Ct, Rule 2.306(a)(1)*].
- If electronic service is made pursuant to the recipient's agreement or local court rules or order, the recipient's time to respond is extended by two court days [*CCP § 1010.6(a)(6), (8)*; see *Cal Rules Ct, Rule 2.250 et seq.*].

7.12[4] Reply Memorandum Should Be Prepared in Response to Opposing Memorandum. A reply memorandum should be prepared if the opposing memorandum raises issues or evidence not sufficiently addressed in the supporting memorandum.



Timing:

Reply papers must be filed, and a copy served on each party, at least five court days before the hearing [*CCP § 1005(b)*]. Service of the reply must be made in a manner reasonably calculated to ensure delivery not later than the close of the business day after the reply is filed [*CCP § 1005(c)*].



Warning:

CCP § 1013, which extends the time within which a right may be exercised or an act may be done based on the manner of service, does not apply to extend the time for filing a reply to papers opposing a motion [*CCP § 1005(b)*].

7.12[5] Counsel Should Attend Hearing on Motion. Counsel for the moving party should plan to make a personal appearance at the hearing on the motion. If counsel fails to appear without having given notice of nonappearance, the court may take the matter off calendar (to be reset only on motion), or the court may rule on the matter [*Cal Rules Ct, Rule 3.1304(d)*].

Exception--Notice of Nonappearance:

A party may give notice that he or she will not appear at the hearing and submit the matter without an appearance unless the court orders otherwise [*Cal Rules Ct, Rule 3.1304(c)*].

Exception--Telephone Appearance:

A party that has provided notice may appear by telephone at a hearing on a noticed motion, unless the

court requires a personal appearance in the particular case [*CCP* § 367.5(b)(3), (4)(c); see *Cal Rules Ct, Rule 3.670(c)(3),(4), (e)(2)*].

Exception--Tentative Ruling:

Counsel should determine whether the court has adopted a procedure of issuing tentative rulings that become final unless a hearing is ordered or requested by a party [see *Cal Rules Ct, Rule 3.1308(a)(1)*]. If so, and the tentative ruling is to grant the requested injunction, counsel need not attend the scheduled hearing unless the court specifically requires attendance or an opposing party has given notice that it intends to appear at the hearing.

7.12[6] Order Must Be Signed, Filed, and Served. If the motion is granted, unless the court otherwise orders, notice of the court's decision or order must be given by the movant (the prevailing party) to all other parties or their attorneys, unless notice is waived by all parties in open court and is entered in the minutes [*CCP* § 1019.5(a)].



Cross Reference:

Submission of proposed order with moving papers, see 7.12[1][f].

Forms:

See 7.22, 7.23.

If the court has not adopted the movant's proposed order, and the parties have not waived notice, the movant must prepare a proposed order reflecting the court's ruling. The proposed order must be mailed or delivered to the opposing party within five days of the ruling, for approval as conforming to the court's ruling. The proposed order will be deemed approved if the opposing party does not object within five days after mailing or delivery [*Cal Rules Ct, Rule 3.1312(a)*].

On expiration of the opposing party's five-day period to object, the movant must promptly transmit the proposed order to the court, together with a summary of any responses of the other parties or a statement that no responses were received [*Cal Rules Ct, Rule 3.1312(b)*].



88 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery

IV. OPPOSING INJUNCTION TO PRESERVE ELECTRONIC EVIDENCE

1-7 MB Practice Guide: CA E-Discovery and Evidence 7.13

7.13 CHECKLIST: Opposing Injunction to Preserve Electronic Evidence.

☐ On receipt of notice of motion for preliminary injunction to preserve electronic evidence, or any other notice that discovery of electronic evidence is likely to be sought:

☐ Advise client not to take any steps that could result in loss or destruction of evidence specified in notice.

Authority:

UMG Recordings, Inc. v. Hummer Winblad Venture Partners (In re Napster, Inc. Copyright Litig.) (ND Cal 2006) 462 F Supp 2d 1060, 1069) ; *Zubulake v. UBS Warburg LLC* (SDNY 2003) 220 FRD 212, 216 ; *Cedars-Sinai Med. Ctr. v. Superior Court* (1998) 18 C4th 1, 12, 74 CR2d 248, 954 P2d 511 ; *Dodge, Warren & Peters Ins. Servs., Inc. v. Riley* (2003) 105 CA4th 1414, 1418-1420, 130 CR2d 385

Discussion:

See 7.05

☐ Contact movant's counsel and offer to meet and confer for purpose of resolving issues relating to preservation and discovery of electronically stored information.

Authority:

Cal Rules Ct, Rule 3.724(8)

Discussion:

See 7.14

☐ If issues raised in motion cannot be resolved by conference between counsel, prepare papers opposing motion, including:

- ☐ Memorandum opposing motion.

Authority:

Cal Rules Ct, Rule 3.1113

Discussion:

See 7.15[1][a]

- ☐ Opposing declarations negating movant's factual allegations of grounds for injunctive relief.

Authority:

CCP § 526(a)(2)-(5)

Discussion:

See 7.15[1][b]

- ☐ File and serve opposing papers.

- ☐ If opposing ex parte application:

Authority:

Cal Rules Ct, Rule 3.1206

Discussion:

See 7.15[2][a]

- ☐ Serve copy of opposing papers on applicant at first reasonable opportunity.

- ☐ File originals of opposing papers at first reasonable opportunity, or if filing before hearing is impracticable, submit opposing papers to judge at hearing on ex parte application.

- ☐ If opposing noticed motion:

Authority:

CCP §§ 1005(b), 1010.6(a)(6)

Discussion:

See 7.15[2][b]

- ☐ File and serve opposing papers at least nine court days before hearing on motion, unless notice of motion was served electronically, in which case time to file and serve opposing papers is extended by two court days.

- ☐ Accomplish service in manner reasonably calculated to ensure delivery not later

than close of next business day after day on which papers are filed.

☐ Attend hearing on motion.



89 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery

IV. OPPOSING INJUNCTION TO PRESERVE ELECTRONIC EVIDENCE

1-7 MB Practice Guide: CA E-Discovery and Evidence 7.14

7.14 Options and Strategies.

As soon as counsel becomes aware of impending litigation that might involve the discovery of electronically stored information possessed by the client, counsel should advise the client to implement procedures to preserve that information pending discovery.

Cross References:

Discussion of parties' duty to preserve electronic evidence, see 7.05.

Planning for discovery of electronic evidence, see *Ch. 4, Planning E-Discovery, 4.03-4.10*.

Best practices for retention of electronically stored information, see *Ch. 16, Establishing Best Practices Regarding Electronically Stored Information*.

Once litigation commences, counsel or client may receive notice that the adverse party is seeking an injunctive order to preserve electronic evidence. This notice may come in the form of a copy of an ex parte application, an order to show cause (combined with a temporary restraining order), or a notice of motion for a preliminary injunction [see *CCP §§ 527(c), 1005(b); Cal Rules Ct, Rules 3.1150, 3.1203(a), 3.1204(a), 3.1206, 3.1300*].

Cross References:

Discussion of ex parte application for temporary restraining order, see 7.11.

Discussion of noticed motion for preliminary injunction, see 7.12.

When such a notice is received, counsel should consider offering to meet and confer with the movant's counsel in an attempt to resolve the issues raised by the application or motion for injunctive relief. A "meet and confer" conference is mandatory in any case [see *Cal Rules Ct, Rule 3.724(8)*], and can be an efficient, cost-effective way to arrive at a mutually acceptable plan for the preservation and discovery of relevant electronic evidence.



Strategic Point:

Counsel opposing a motion for a preliminary injunction should consider stipulating to a lesser form of

relief, because that may convince the court to deny the motion for more drastic measures. For example, a party might stipulate that it has and will preserve information, but oppose inspection of the information by opposing counsel without a document request and prior review by the producing party's counsel.

➡ **Cross Reference:**

Notice that discovery of electronically stored information is reasonably likely to be sought, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferring, and Case Management Conference*, 5.09-5.13

If the proposed injunctive order is not acceptable to the client, and the issues raised by the request for injunctive relief cannot be resolved by agreement of the parties, counsel should prepare, file, and serve papers opposing the motion.

➡ **Cross Reference:**

Preparation, filing, and service of opposing papers, see 7.15.



90 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery

IV. OPPOSING INJUNCTION TO PRESERVE ELECTRONIC EVIDENCE

1-7 MB Practice Guide: CA E-Discovery and Evidence 7.15

7.15 Opposing Application or Motion for Injunction to Preserve Electronic Evidence.

7.15[1] Preparing Opposing Papers.

7.15[1][a] Opposing Party Should Prepare Memorandum. A party opposing an application or motion for an injunctive order to preserve electronic evidence should prepare a memorandum [see *Cal Rules Ct, Rule 3.1113*] presenting the arguments against the issuance of injunctive relief.

Potential arguments against issuance of an injunction include:

- Ordinary discovery procedures are sufficient to preserve the information necessary for the case, and extraordinary issuance of an injunction is not required [see, e.g., *Pueblo of Laguna v. United States (Fed Cl 2004) 60 Fed Cl 133, 135* ; *Daimler Truck N. Am. LLC v. Younessi (WD Wash June 20, 2008) 2008 US Dist LEXIS 86022, at *6-*9* (noting extraordinary nature of allowing an opposing party to search through a responding party's computer hard drives in search of a limited class of documents); *Hedenburg v. Aramark Am. Food Servs. (WD Wash Jan. 17, 2007) 2007 US Dist LEXIS 3443* (mirror image of computer not allowed just to seek evidence impeaching plaintiff, analogizing that a party could not search property for a lost paper diary)].
- The risks of disclosure of trade secrets or privileged information outweigh the benefits of allowing access to the electronically stored information sought [*Daimler Truck N. Am. LLC v. Younessi (WD Wash June 20, 2008) 2008 US Dist LEXIS 86022, at *7-*9* (denying motion to quash subpoena)].
- An injunction would impose unnecessary burdens on the respondent.

Example:

If the electronic evidence sought to be preserved is privileged material, it will not be within the permissible scope of discovery [CCP § 2017.010]. The privileged nature of the evidence therefore can serve as a basis for arguing that the court should not grant an injunction to preserve the evidence, because the movant will be unable to show a likelihood of success on the merits. However, unless the discovery sought is from an attorney, it is unlikely that all of the information sought by the movant will be privileged, so limitations to protect privileged data amongst other data are more likely. In the context

of a requested injunction to preserve evidence pending discovery, the "merits" concerns the merits of the question of discoverability of the evidence [*Dodge, Warren & Peters Ins. Servs., Inc. v. Riley* (2003) 105 CA4th 1414, 1420-1421, 130 CR2d 385] . A similar argument could be based on the proposition that the information sought to be preserved is not admissible and is not likely to lead to the discovery of admissible evidence, although this proposition is more difficult to establish than a straightforward claim of evidentiary privilege [see CCP § 2017.010; *Dodge, Warren & Peters Ins. Servs., Inc. v. Riley* (2003) 105 CA4th 1414, 1421, 130 CR2d 385] .

7.15[1][b] Opposing Party Should Prepare Declarations. The opposing memorandum should be accompanied by one or more declarations, containing competent testimony based on personal knowledge, negating the movant's asserted grounds for injunctive relief [see CCP § 526(a)], such as the following:

- The factual basis for a claim that the information sought to be preserved is privileged and therefore not subject to discovery [see CCP § 2017.010].
- The opposing party is not doing, threatening, procuring, or allowing to be done any act that would result in the loss or destruction of relevant evidence [CCP § 526(a)(3); see *Dodge, Warren & Peters Ins. Servs., Inc. v. Riley* (2003) 105 CA4th 1414, 1418-1419, 130 CR2d 385] .
- The measures that respondent has undertaken to preserve evidence will preserve the necessary evidence for the case.
- The loss or destruction of the evidence sought to be preserved would not cause great or irreparable injury to the applicant or movant, because it would not prevent the applicant or movant from presenting relevant evidence on his or her claim or defense in the litigation [CCP § 526(a)(2)]. For example, it could be argued that the evidence would be duplicative or too burdensome to preserve in light of the issues in the case.
- The evidence sought to be preserved is not critical to the applicant's ability to prove his or her claim or defense, and pecuniary compensation for the inadvertent loss of any evidence would afford adequate relief [CCP § 526(a)(4), (5)].
- The issuance of the requested injunctive relief would cause great or irreparable harm to the opposing party, for example, by interrupting the opposing party's ability to conduct its business operations, or by causing the disclosure of the opposing party's trade secrets or other confidential and proprietary business information [see *Dodge, Warren & Peters Ins. Servs., Inc. v. Riley* (2003) 105 CA4th 1414, 1421, 130 CR2d 385 ; see also CCP § 2017.020(a)].



Strategic Point:

To the extent possible, conclusory allegations of harm should be avoided, and detailed information regarding the specific consequences should be provided [see *OpenTV v. Liberate Techs.* (ND Cal 2003) 219 FRD 474 ("[h]ere, the parties failed to estimate or indicate the cost of production, the amount in controversy, or the resources available to each party. In the joint letter, OpenTV makes conclusory statements that the cost of production is small in comparison to the amount in controversy and in comparison to the resources available to both parties. Liberate makes no statements to the contrary")].

7.15[2] Filing and Serving Opposing Papers.

7.15[2][a] Opposing Party Must Serve Opposition to Ex Parte Application. An opposing party appearing at the ex parte hearing must serve any written opposition on all other appearing parties at the first reasonable opportunity. Absent exceptional circumstances, no hearing may be conducted unless service has been made [*Cal Rules Ct, Rule 3.1206*].

7.15[2][b] Opposing Party Must Serve Opposition to Noticed Motion. Papers opposing a noticed motion generally must be filed and served at least nine court days before the hearing [*CCP § 1005(b)*]. Service of the opposing papers must be made in a manner reasonably calculated to ensure delivery not later than the close of the business day after the papers are filed [*CCP § 1005(c)*].



Warning:

CCP § 1013, which extends the time within which a right may be exercised or an act may be done if that time is triggered by service of a document served by mail, express mail, overnight delivery, or facsimile transmission, does not apply to extend the time for filing papers opposing a noticed motion [*CCP § 1005(b)*].

Distinguish:

CCP § 1005(b), which makes *CCP § 1013* inapplicable to extend the time for filing and serving opposition to noticed motions, does not mention *CCP § 1010.6*, which authorizes electronic filing and service of documents pursuant to the recipient's agreement or local court rules or order. Therefore, it appears that if electronic service of the noticed motion was made, the time to file and serve opposing papers is extended by two court days [*CCP § 1010.6(a)(6),(8)*; see *Cal Rules Ct, Rule 2.250 et seq.*].



91 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery
V. FORMS

*1-7 MB Practice Guide: CA E-Discovery and Evidence 7.16***7.16 Ex Parte Application for Temporary Restraining Order and Order to Show Cause.**

Ex Parte Application for Temporary Restraining Order and Order to Show Cause.

Tom Doe

California Bar Number 987654

100 North Main St., Suite 200

Farallon City, California 90000

Phone: 555-555-5555

Attorney for Plaintiff, John Smith

SUPERIOR COURT OF CALIFORNIA,

COUNTY OF FARALLON

	)	
	)	No. _____
	)	PLAINTIFF'S EX PARTE APPLICATION
	)	FOR TEMPORARY RESTRAINING ORDER
	)	AND ORDER TO SHOW
	)	CAUSE REGARDING
John Smith, Plaintiff, vs. Mary Jones Enterprises,	)	PRELIMINARY INJUNCTION
Inc., Defendant.	)	Date: _____
	)	Time: _____
	)	Location: _____
	)	Judge: _____
	)	Date Action Filed: _____
	)	Trial Date: _____
	)	

Plaintiff, John Smith, hereby applies for a temporary restraining order prohibiting Defendant, Mary Jones Enterprises, Inc., and its agents, servants, employees, and representatives from _____ [describe acts, e.g., destroying, concealing, or disposing of any documents, paper, electronic files, or other material belonging to Plaintiff; or containing or derived from Plaintiff's trade secrets or confidential or proprietary information; or altering, deleting, removing,

erasing, reusing, or writing over in any respect any documents, computer files (including, but not limited to e-mails, hard drives, disk drives, Zip drives, and backup tapes, disks, or drives), data, drafts, or other materials relating in any way to Plaintiff (*or identify relevant information by describing transactions, events, and dates*), and an order to show cause why a preliminary injunction should not be granted enjoining Defendant and its agents, servants, employees, and representatives from performing these acts during the pendency of this action.

[*Optional*: Plaintiff further applies for an order of this Court requiring that Defendant make the following items available for imaging and preservation by _____ (*name*), acting as an independent expert under the supervision of this Court: all computer (laptop and/or desktop) and other electronic storage devices, including but not limited to external hard drives, Zip drives, memory sticks, jump drives, CDs, DVDs, floppy disks, Blackberries, and other PDAs or cell phones with text messaging or electronic mail capabilities, used by Defendant at Defendant's offices or home since _____ (*date*)].

[*Optional*: Plaintiff further applies for an order of this Court requiring that Defendant make all documents, things, or other materials obtained from or belonging to plaintiff, derived from Plaintiff's trade secrets or confidential or proprietary information, available for copying.]

Plaintiff has not previously applied for similar relief in this action.

[*Optional*: Contemporaneous with the filing of this Motion, Plaintiff has also filed, and incorporates by reference, its original Complaint, memorandum in support of this motion, and declaration(s) of _____ (*name[s]*).]

This application is made on the ground(s) that _____ [*specify one or more grounds listed in CCP § 526(a), e.g., a failure to enjoin the acts described above would result in the irretrievable loss of evidence relevant to this action*], and on the further ground that great and irreparable injury will result to Plaintiff before the matter can be heard on notice. In its attached memorandum and supporting declarations, Plaintiff has presented evidence that _____ [*specify, e.g., Defendants have repeatedly misappropriated Defendants' trade secret and other confidential information, and have previously deleted their electronic files*]. If the requested relief is not granted, Plaintiff will be immediately and irreparably injured by _____ [*specify, e.g., the further loss of its trade secrets and loss of evidence supporting the allegations in its Complaint*].

Based on all the evidence and authorities set forth in Plaintiff's supporting memorandum and declarations, Plaintiff has clearly demonstrated its entitlement to a temporary restraining order, and therefore respectfully requests that the Court grant this ex parte motion for a temporary restraining order prohibiting the destruction of evidence [and requiring imaging of electronic media].

Counsel for Defendant is Jane Lee, whose address is 50 South Main St., Suite 100, Farallon City, California 90000, and whose telephone number is 555-999-9999.

Dated: _____

Respectfully submitted,

_____ [*signature*]

Tom Doe

Attorney for Plaintiff, John Smith

NOTES:

Authority:

CCP §§ 526(a), 527(c); *Dodge, Warren & Peters Ins. Servs., Inc. v. Riley* (2003) 105 CA4th 1414, 1418-1419, 130 CR2d 385

Checklist:

See 7.09

Discussion:

See 7.11[1][a]

Related Form for Declaration Supporting Ex Parte Application:

See 7.17

Related Form for Declaration Supporting Injunctive Relief:

See 7.18

Related Form for Order:

See 7.19



92 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery
V. FORMS

1-7 MB Practice Guide: CA E-Discovery and Evidence 7.17

7.17 Declaration in Support of Ex Parte Application for Temporary Restraining Order and Order to Show Cause.

Declaration in Support of Ex Parte Application for Temporary Restraining Order and Order to Show Cause.

Tom Doe

California Bar Number 987654

100 North Main St., Suite 200

Farallon City, California 90000

Phone: 555-555-5555

Attorney for Plaintiff, John Smith

SUPERIOR COURT OF CALIFORNIA,

COUNTY OF FARALLON

John Smith, Plaintiff, vs. Mary Jones Enterprises,
Inc., Defendant.

)
) No. ____
) DECLARATION IN SUPPORT OF
) PLAINTIFF'S EX PARTE APPLICATION FOR
) TEMPORARY RESTRAINING ORDER
) AND ORDER TO SHOW
) CAUSE REGARDING
) PRELIMINARY INJUNCTION
) Date: _____
) Time: _____
) Location: _____
) Judge: _____
) Date Action Filed: _____
) Trial Date: _____
)

1. I am an attorney at law duly admitted to practice before all the courts of the state of California and the attorney of record in this matter for the Plaintiff.

2. This declaration is made in support of Plaintiff's application for a temporary restraining order and an order to show cause regarding preliminary injunction to prevent Defendant and its agents, servants, employees, and representatives from _____ [*describe acts, e.g., destroying, concealing, or disposing of any documents, paper, or electronic files or other material belonging to Plaintiff; or containing or derived from Plaintiff's trade secrets or confidential or proprietary information; or altering, deleting, removing, erasing, reusing, or writing over in any respect any documents, computer files (including, but not limited to e-mails, hard drives, disk drives, Zip drives, and backup tapes, disks, or drives), data, drafts, or other things relating in any way to Plaintiff (or identify relevant information by describing transactions, events, and dates)*] , and an order to show cause why a preliminary injunction should not be granted enjoining Defendant and its agents, servants, employees, and representatives from performing these acts during the pendency of this action.

3. Counsel for Defendant is Jane Lee, whose address is 50 South Main St., Suite 100, Farallon City, California 90000, and whose telephone number is 555-999-9999.

4. Great and irreparable injury will result to Plaintiff before this matter can be heard on notice because _____ [*e.g., the electronically stored information described above is pivotal to the Plaintiff's claim, and Defendant's counsel has informed me that Defendant will not agree to preserve the information and will delete that information at the Defendant's next weekly computer backup; if necessary, provide facts showing irreparable injury through declarations of other persons with personal knowledge*].

[EITHER]

5. On _____ [date], at _____ [time], I informed Jane Lee, Defendant's counsel, of the date, time, and place that the above application for a temporary restraining order and order to show cause would be made. Ms. Lee informed me that Defendant _____ [would or would not] appear and oppose the application [*or describe other response of defense counsel to notice of ex parte application*].

[OR]

5. On _____ [date], I attempted to inform Jane Lee, Defendant's counsel, of the date, time, and place that the above application for a temporary restraining order and order to show cause. I was unable to do so even though _____ [*describe efforts made, e.g., I telephoned Ms. Lee's office at _____ (time), and again at _____ (time)*].

[OR]

5. Notice to Defendant and its counsel of record of the above application for a temporary restraining order and an order to show cause should not be required because I have reason to believe that Defendant may destroy the electronic evidence described in Paragraph 2 above. Specifically, the evidence described in Paragraph 2 is vital to Plaintiff's cause of action in that _____ [*set forth facts within personal knowledge of declarant establishing that electronic evidence sought is essential to plaintiff's claim*]. Further, _____ [*set forth facts within personal knowledge of declarant indicating, e.g., that defendant has motive to destroy evidence or that defendant has destroyed other relevant evidence; if necessary, provide this information through declarations of other persons with personal knowledge*].

[CONTINUE]

I declare under penalty of perjury under the laws of the state of California that the foregoing is true and correct.

Dated: _____
_____ [signature]
[typed name]

NOTES:

Authority:

CCP §§ 526, 527(c); *Dodge, Warren & Peters Ins. Servs., Inc. v. Riley* (2003) 105 CA4th 1414, 1418-1419, 130 CR2d 385

Checklist:

See 7.09

Discussion:

See 7.11[1][b]

Related Form for Ex Parte Application:

See 7.16

Related Form for Declaration Supporting Injunctive Relief:

See 7.18

Related Form for Order:

See 7.19



93 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery
V. FORMS

1-7 MB Practice Guide: CA E-Discovery and Evidence 7.18

7.18 Declaration Supporting Application or Motion for Injunctive Relief.

Declaration Supporting Application or Motion for Injunctive Relief.

Tom Doe

California Bar Number 987654

100 North Main St., Suite 200

Farallon City, California 90000

Phone: 555-555-5555

Attorney for Plaintiff, John Smith

SUPERIOR COURT OF CALIFORNIA,

COUNTY OF FARALLON

	)	
	)	No. _____
	)	DECLARATION OF
John Smith, Plaintiff, vs. Mary Jones Enterprises,	)	_____ [e.g., JOHN SMITH]
Inc., Defendant.	)	SUPPORTING PLAINTIFF'S
	)	[APPLICATION or MOTION]
	)	FOR INJUNCTIVE RELIEF
	)	

1. I am _____ [e.g., the Plaintiff in this action].

2. _____ [Set forth facts showing that adverse party is doing, threatening, about to do, procuring, or allowing to be done some act that would result in loss or destruction of relevant evidence, thus rendering eventual discovery request ineffectual, e.g., Defendant's routine computer backup procedure involves the overwriting of its backup media; this procedure, if not enjoined, will result in the irretrievable loss of information pertaining to my claim that Defendant misappropriated and used trade secrets and other confidential and proprietary information owned by me, without my knowledge, permission, or consent, and the loss of that evidence would render any eventual discovery request for that evidence ineffectual, because there is no other source of that information].

3. _____ [Set forth facts showing that loss or destruction of electronically stored evidence in possession of adverse party would cause plaintiff great or irreparable injury, e.g., Without the electronically stored information described above, I will be unable to prove my claim that Defendant misappropriated and used trade secrets and other confidential and proprietary information. Defendant's internal records, e-mails and other communications, and other data relating to the acquisition, possession, and use of those trade secrets and information are the best source of information regarding Defendant's activities relating to this Complaint, and are essential to prove the allegations of the Complaint. These materials exist only on Defendant's computer systems and other electronic media and will be lost if Defendant destroys, deletes, or overwrites those materials, making it difficult or impossible for Plaintiff to prove the allegations in the Complaint].

4. _____ [Set forth facts showing inadequacy of legal remedy for loss of evidence, e.g., If the loss of the electronically stored information described above prevents me from proving my claim, pecuniary compensation would be inadequate to compensate me for the loss, since the relief I seek in this action includes a permanent injunction against the defendant's conduct, and the monetary value of that relief would be extremely difficult to calculate].

I declare under penalty of perjury under the laws of the state of California that the foregoing is true and correct.

Dated: _____
_____ [signature]
[typed name]

NOTES:

Authority:

CCP § 526(a)(2)-(5)

Checklist:

See 7.09

Discussion:

See 7.11[1][c]

Related Form for Ex Parte Application:

See 7.16

Related Form for Declaration Supporting Ex Parte Application:

See 7.17

Related Form for Motion for Preliminary Injunction:

See 7.20

Related Forms of Orders:

See 7.19, 7.22, 7.23



94 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery
V. FORMS

*1-7 MB Practice Guide: CA E-Discovery and Evidence 7.19***7.19 Order to Show Cause and Temporary Restraining Order Directing Preservation of Electronic Evidence.**

Order to Show Cause and Temporary Restraining Order Directing Preservation of Electronic Evidence.
SUPERIOR COURT OF CALIFORNIA,
COUNTY OF FARALLON

John Smith, Plaintiff, vs. Mary Jones Enterprises,
Inc., Defendant.

)
)
) No. _____
) ORDER TO SHOW CAUSE
) AND TEMPORARY
) RESTRAINING ORDER
)

Application has been made by Plaintiff, John Smith, and it appears to the Court that unless the temporary restraining order prayed for is granted, great or irreparable injury will result to Plaintiff before the matter can be heard on notice. Therefore, the Court grants an order to show cause for a preliminary injunction and a temporary restraining order.

IT IS ORDERED that Defendant, Mary Jones Enterprises, Inc., appear in [Department or Division _____ of] this court, located at 1 North Main Street, Farallon City, California, on _____ [date], at _____ [time], or as soon thereafter as the matter may be heard, then and there to show cause, if any, why defendant and its agents, servants, employees, and representatives should not be enjoined and restrained by order of this Court during the pendency of this action from committing or performing, directly or indirectly, any and all of the following acts:

_____ [describe acts, e.g., Destroying, concealing, or disposing of any documents, paper, or electronic files or other material belonging to Plaintiff; or containing or derived from Plaintiff's trade secrets or confidential or proprietary information; or altering, deleting, removing, erasing, reusing, or writing over in any respect any documents, computer files, (including, but not limited to e-mails, hard drives, disk drives, Zip drives, and backup tapes, disks, or drives), data, drafts, or other things relating in any way to Plaintiff, until such time as those materials may be turned over it discovery or until further order of this Court].

[Optional: IT IS FURTHER ORDERED THAT Defendant shall appear, at the time and place indicated above, and show cause, if any, why Defendant should not be ordered to make the following items available for imaging and preservation by _____ (name), acting as an independent expert under the supervision of this Court: all computer (laptop and/or desktop) and other electronic storage devices, including but not limited to external hard drives, Zip drives, memory sticks, jump drives, CDs, DVDs, floppy disks, Blackberries, and other PDAs or cell phones with text messaging or electronic mail capabilities, used by Defendant at Defendant's offices or home since _____ (date)].

[Optional: IT IS FURTHER ORDERED THAT Defendant shall appear, at the time and place indicated above, and show cause, if any, why Defendant should not be ordered to make all documents, things, or other materials obtained from or belonging to plaintiff, derived from Plaintiff's trade secrets or confidential or proprietary information, available for copying.]

IT IS FURTHER ORDERED that:

a. Plaintiff shall serve this order to show cause on Defendant in the following time and manner:

_____ .

b. Proof of service must be delivered to this Court on: _____ .

c. The parties shall adhere to the following briefing schedule: _____ .

[d. The temporary restraining order stated below shall expire on: _____ .]

IT IS FURTHER ORDERED that, pending the hearing and determination of the order to show cause, from this day forward Defendant and its officers, agents, employees, and representatives, and all persons acting in concert or participating with them, are hereby restrained and enjoined from engaging in or performing, directly or indirectly, any and all of the following acts:

[describe acts, e.g., Destroying, concealing, or disposing of any documents, paper, or electronic files or other material belonging to Plaintiff; or containing or derived from Plaintiff's trade secrets or confidential or proprietary information; or altering, deleting, removing, erasing, re-using, or writing over in any respect any documents, computer files, (including, but not limited to e-mails, hard drives, disk drives, Zip drives, and backup tapes, disks, or drives), data, drafts, or other things relating in any way to Plaintiff, until such time as those materials may be turned over in discovery or until further order of this Court].

IT IS FURTHER ORDERED that copies of the complaint, ex parte application for this temporary restraining order, memorandum, attached declaration(s), and this order to show cause and temporary restraining order be served on Defendant not later than _____ [date].

[If counsel for plaintiff knows that court will require bond before issuing temporary restraining order, include order fixing bond, e.g., Bond on this temporary restraining order is fixed in the sum of \$ _____. If counsel for plaintiff does not know in advance that court will require bond before issuing temporary restraining order, body of order should not include reference to bond, which can be added later.]

Let the above order issue [on plaintiff's filing a bond in the sum of \$ _____].

Dated: _____

_____ [signature]

Judge of the Superior Court

NOTES:

Authority:

CCP § 527(c), (d)

Checklist:

See 7.09

Discussion:

See 7.11[1][f], [5]

Related Form for Ex Parte Application:

See 7.16

Related Form for Declaration Supporting Ex Parte Application:

See 7.17



95 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery
V. FORMS

*1-7 MB Practice Guide: CA E-Discovery and Evidence 7.20***7.20 Notice of Motion and Motion for Preliminary Injunction to Preserve Electronic Evidence.**

Notice of Motion and Motion for Preliminary Injunction to Preserve Electronic Evidence.

Tom Doe

California Bar Number 987654

100 North Main St., Suite 200

Farallon City, California 90000

Phone: 555-555-5555

Attorney for Plaintiff, John Smith

SUPERIOR COURT OF CALIFORNIA,

COUNTY OF FARALLON

	)	
	)	No. _____
	)	NOTICE OF MOTION AND MOTION
	)	FOR PRELIMINARY INJUNCTION
	)	TO PRESERVE
John Smith, Plaintiff, vs. Mary Jones Enterprises,	)	ELECTRONICALLY STORED INFORMATION
Inc., Defendant.	)	Date: _____
	)	Time: _____
	)	Location: _____
	)	Judge: _____
	)	Date Action Filed: _____
	)	Trial Date: _____
	)	

To defendant, Mary Jones Enterprises, Inc., and its attorney of record:

NOTICE IS HEREBY GIVEN that, on _____ [date], at _____ [time], or as soon thereafter as the matter may be heard, in [_____ (Department or Division) _____ of] this Court, located at 1 North Main Street, Farallon City, California, Plaintiff, John Smith, will, and hereby does, move

for an order of this Court prohibiting Defendant, Mary Jones Enterprises, Inc., and its agents, servants, employees, and representatives, from _____ [*describe acts, e.g., destroying, concealing, or disposing of any documents, paper, or electronic files or other material belonging to Plaintiff; or containing or derived from Plaintiff's trade secrets or confidential or proprietary information; or altering, deleting, removing, erasing, reusing, or writing over in any respect any documents, computer files (including, but not limited to e-mails, hard drives, disk drives, Zip drives, and backup tapes, disks, or drives), data, drafts, or other things relating in any way to Plaintiff (or identify relevant information by describing transactions, events, and dates)*].

[*Optional*: Plaintiff also will, and hereby does, move for an order of this Court requiring that Defendant make the following items available for imaging and preservation by _____ (*name*), acting as an independent expert under the supervision of the Court: all computer (laptop and/or desktop) and other electronic storage devices, including but not limited to external hard drives, Zip drives, memory sticks, jump drives, CDs, DVDs, floppy disks, Blackberries, and other PDAs or cell phones with text messaging or electronic mail capabilities, used by Defendant at Defendant's offices or home since _____ (*date*)].

[*Optional*: Plaintiff also will, and hereby does, move for an order of this Court requiring that Defendant make all documents, things, or other materials obtained from or belonging to plaintiff, derived from Plaintiff's trade secrets or confidential or proprietary information, available for copying.]

The motion is made on the ground(s) that _____ [*specify one or more grounds listed in CCP § 526(a), e.g., a failure to enjoin the acts described above would result in the irretrievable loss of evidence relevant to this action*].

The motion is based on this notice of motion, the accompanying declaration of Plaintiff, the accompanying supporting memorandum, the records and file herein, and such evidence as may be presented at the hearing on the motion.

Dated: _____

Respectfully submitted,

_____ [*signature*]

Tom Doe

Attorney for Plaintiff, John Smith

NOTES:

Authority:

CCP §§ 526(a)(2)-(5), 527(a), 1005(b); Cal Rules Ct, Rules 3.1112(a), 3.1150(a)

Checklist:

See 7.09

Discussion:

See 7.12[1][a]

Related Form for Declaration Supporting Injunctive Relief:

See 7.18

Related Forms for Orders:

See 7.22, 7.23



96 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery
V. FORMS

*1-7 MB Practice Guide: CA E-Discovery and Evidence 7.21***7.21 Declaration Opposing Motion for Preliminary Injunction to Preserve Electronic Evidence.**

Declaration Opposing Motion for Preliminary Injunction to Preserve Electronic Evidence.

Jane Lee

California Bar Number 123456

50 South Main St., Suite 100

Farallon City, California 90000

Phone: 555-999-9999

Attorney for Defendant, Mary Jones Enterprises, Inc.

SUPERIOR COURT OF CALIFORNIA,

COUNTY OF FARALLON

	)	
	)	No. _____
John Smith, Plaintiff, vs. Mary Jones Enterprises,	)	DECLARATION OF
Inc., Defendant.	)	_____ [e.g., MARY JONES] OP-
	)	POSING
	)	MOTION FOR
	)	INJUNCTIVE RELIEF

1. I am _____ [e.g., the Chief Executive officer of the Defendant in this action].

2. I have read Plaintiff's Motion for Preliminary Injunction to Preserve Electronically Stored Information and the papers submitted in support of that motion. Except as admitted below [, and except as to those allegations of which I have no information or belief], each and every allegation of the declaration(s) submitted in support of Plaintiff's motion is false.

3. I admit that _____ [set forth admissions of movant's factual allegations as appropriate, e.g., Defendant's mainframe computer generated an electronic record of e-mails sent or received by Defendant's employees on Defendant's computer system between _____ and _____ (dates), as alleged in the declaration of _____ (name)].

4. I have no information or belief as to the truth of the allegation(s) that _____ [*set forth movant's factual allegations that declarant can neither confirm nor deny, e.g., Defendant's mainframe computer contains any e-mails or other stored materials containing information about Plaintiff's business or otherwise relevant to the allegations in Plaintiff's complaint.*]

5. Contrary to the allegation(s) made in the declaration of _____ [*name*], it is not true that _____ [*set forth movant's factual allegations that are denied, e.g., Defendant's e-mails are routinely deleted after six months.*] [*If appropriate, set forth factual allegations disproving movant's factual allegations, e.g., In fact, under Defendant's routine backup procedure, Defendant's e-mails are copied onto electronic storage media and permanently maintained at an offsite archiving facility.*]

6. If the Court grants the preliminary injunction requested by Plaintiff, Defendant will suffer great harm, in that _____ [*e.g., Defendant's normal business procedures will be interrupted and hampered, and the smooth operation of Defendant's mainframe computer will be compromised, if Defendant is enjoined from copying and moving old e-mails and other documents that are no longer needed in Defendant's regular course of business onto separate storage media.*]

7. It is not true that Plaintiff will suffer irreparable harm if the requested injunction is not granted, because _____ [*e.g., Plaintiff will have another source of the relevant electronically stored information; specifically, records of any relevant e-mails and other electronically stored information can be retrieved from Defendant's backup storage media.*]

8. It is not true that Plaintiff will have no adequate remedy at law if the relevant electronically stored information is lost. Defendant is solvent and is capable of responding to any judgment for the damages claimed in this action and particularly for any damages arising from the inadvertent loss of the relevant electronically stored information.

I declare under penalty of perjury under the laws of the state of California that the foregoing is true and correct.

Dated: _____
 _____ [*signature*]
 [*typed name*]

NOTES:

Authority:

CCP § 527(e)

Checklist:

See 7.13

Discussion:

See 7.15[1][b]

Related Form for Declaration Supporting Injunctive Relief:

See 7.18



97 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery
V. FORMS

1-7 MB Practice Guide: CA E-Discovery and Evidence 7.22

7.22 Order--Preliminary Injunction Directing Preservation of Electronic Evidence.

Order--Preliminary Injunction Directing Preservation of Electronic Evidence.
SUPERIOR COURT OF CALIFORNIA,
COUNTY OF FARALLON

John Smith, Plaintiff, vs. Mary Jones Enterprises,
Inc., Defendant.

)
)
)
)

No. ____
ORDER--PRELIMINARY INJUNCTION

The motion of Plaintiff, John Smith, for a preliminary injunction came on regularly for hearing by the Court this date in accordance with _____ [an order to show cause issued by this court on _____ (date) or Plaintiff's noticed motion]. Plaintiff appeared by counsel Tom Doe; Defendant appeared by counsel Jane Lee.

On proof made to the Court's satisfaction, and good cause appearing:

IT IS ORDERED that during the pendency of this action the Defendant and its officers, agents, employees, and representatives, and all persons acting in concert or participating with them, are hereby restrained and enjoined from engaging in or performing, directly or indirectly, any and all of the following acts:

[*describe acts, e.g.*, Destroying, concealing, or disposing of any documents, paper, or electronic files or other material belonging to Plaintiff; or containing or derived from Plaintiff's trade secrets or confidential or proprietary information; or altering, deleting, removing, erasing, reusing, or writing over in any respect any documents, computer files (including, but not limited to e-mails, hard drives, disk drives, Zip drives, and backup tapes, disks, or drives), data, drafts, or other things relating in any way to Plaintiff, until such time as those materials may be turned over in discovery or until further order of this Court].

IT IS FURTHER ORDERED that, before this order shall take effect, Plaintiff must file a written undertaking in the sum of \$_____, as required by *Code of Civil Procedure Section 529* for the purpose of indemnifying Defendant for any damage it may sustain by reason of this preliminary injunction if the Court finally decides that Plaintiff is not entitled to

it.

Dated: _____
_____ [signature]

Judge of the Superior Court

NOTES:

Authority:

CCP §§ 527, 529

Checklist:

See 7.09

Discussion:

See 7.07[3][a], 7.12[1][f], [6]

Related Forms for Order:

See 7.23



98 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 7 Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery
V. FORMS

*1-7 MB Practice Guide: CA E-Discovery and Evidence 7.23***7.23 Order--Preliminary Injunction Directing Seizure and Copying of Electronic Evidence.**

Order--Preliminary Injunction Directing Seizure and Copying of Electronic Evidence.
SUPERIOR COURT OF CALIFORNIA,
COUNTY OF FARALLON

John Smith, Plaintiff, vs. Mary Jones Enterprises,	)	
Inc., Defendant.	)	No. _____
	)	ORDER--PRELIMINARY INJUNCTION
	)	

The motion of Plaintiff, John Smith, for a preliminary injunction came on regularly for hearing by the Court this date in accordance with _____ [an order to show cause issued by this court on _____ (date) or Plaintiff's noticed motion]. Plaintiff appeared by counsel Tom Doe; Defendant appeared by counsel Jane Lee.

On proof made to the Court's satisfaction, and good cause appearing:

IT IS ORDERED that _____ [name of independent expert] is appointed to access and make electronic copies of the following electronically stored information that is currently in the possession of defendant: All computer (laptop and/or desktop) and other electronic storage devices, including but not limited to external hard drives, Zip drives, memory sticks, jump drives, CDs, DVDs, floppy disks, Blackberries, and other PDAs or cell phones with text messaging or electronic mail capabilities, used by Defendant at Defendant's offices or home since _____ (date)]. Defendant shall permit _____ [name of independent expert] to have access to and copy the described electronically stored information on _____ [date] at _____ [time].

IT IS FURTHER ORDERED that _____ [name of independent expert] shall maintain custody of the copies so made until further order of this Court.

[Optional: IT IS FURTHER ORDERED that Defendant shall make all documents, things, or other materials obtained from or belonging to plaintiff, derived from Plaintiff's trade secrets or confidential or proprietary information, available

for copying.]

IT IS FURTHER ORDERED that the reasonable fees and expenses of _____ [*name of independent expert*] incurred in performing the duties described in this order shall be borne by _____ [Plaintiff or Defendant].

IT IS FURTHER ORDERED that until _____ [*name of independent expert*] has completed the process of making the copies described above, the Defendant and its officers, agents, employees, and representatives, and all persons acting in concert or participating with them, are hereby restrained and enjoined from engaging in or performing, directly or indirectly, any and all of the following acts:

[*describe acts, e.g., Destroying, concealing, or disposing of any documents, paper, or electronic files or other material belonging to Plaintiff; or containing or derived from Plaintiff's trade secrets or confidential or proprietary information; or altering, deleting, removing, erasing, reusing, or writing over in any respect any documents, computer files (including, but not limited to e-mails, hard drives, disk drives, Zip drives, and backup tapes, disks, or drives), data, drafts, or other things relating in any way to Plaintiff.*]

IT IS FURTHER ORDERED that, before this order shall take effect, Plaintiff must file a written undertaking in the sum of \$ _____, as required by *Code of Civil Procedure Section 529* for the purpose of indemnifying Defendant for any damage it may sustain by reason of this preliminary injunction if the Court finally decides that Plaintiff is not entitled to it.

Dated: _____
 _____ [*signature*]

Judge of the Superior Court

NOTES:

Authority:

CCP §§ 527, 529

Checklist:

See 7.09

Discussion:

See 7.07[3][b], 7.12[1][f], [6]

Related Form for Order:

See 7.22



99 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court

1-8 MB Practice Guide: CA E-Discovery and Evidence 8.syn

§ 8.syn Synopsis to Chapter 8: Responding to Electronic Discovery Demands in California Court

8.01 Scope.

8.02 Objective and Strategy.

8.03 CHECKLIST: Developing Response Strategy.

8.04 Options and Strategies.

8.05 Responding Party's Counsel Should Contact Client Immediately to Begin Formulating Response Strategy.

8.06 Counsel Should Analyze Request.

8.06[1] Counsel Should Determine If ESI Exists and Is In Client's Possession.

8.06[2] Counsel Should Evaluate Whether Request Is Overbroad or Unduly Burdensome.

8.07 Counsel Should Assess Options for Responding to Each Item or Category in Request.

8.07[1] Party May Produce Information As Requested.

8.07[2] Party May Object to Production in Whole or in Part.

8.07[3] Party May Seek a Protective Order.

8.08 Cost Shifting or Sharing Can Be Sought.

8.09 Respondent Must Decide Form in Which ESI Will Be Produced.

8.09[1] Respondent May Produce ESI in Form Specified in Request.

8.09[2] Respondent May Produce ESI in Form in Which It Is Maintained in Ordinary Course of Business.

8.09[3] Respondent May Produce ESI in a Form That Is Reasonably Usable.

8.10 Respondent Should Address Issues of Privileged and Confidential Information.

8.10[1] Counsel Should Review ESI for Privileged and Confidential Information.

8.10[2] Inadvertent Disclosure of Privileged Information May Result in Waiver of Privilege.

8.10[3] Producing Party Must Immediately Notify the Receiving Party of Any Inadvertent Disclosure of Privileged Information.

8.10[4] Receiving Party Must Promptly Return to Sender Privileged Information.

8.11 Responsive Documents Must Be Produced in Timely Manner.

8.12 CHECKLIST: Preparing Written Response to Electronic Discovery Request.

8.13 Options and Strategy.

8.14 Making a Timely Response to Electronic Discovery and Inspection Request.

8.15 Failure to Serve Timely Response May Result in Monetary and Other Sanctions.

8.16 Response Must Be Properly Formatted.

8.17 Response Must Address Each Item or Category in Demand.

8.18 Responses Must Be Clearly Identified.

8.19 Response Must Include Statement of Compliance or Inability to Comply.

8.19[1] Contents of Statement of Compliance.

8.19[2] Contents of Statement of Noncompliance.

8.20 Response Must State Form of Production.

8.21 Any Applicable Objections to Request for Production of ESI Should Be Stated.

8.22 Response Must Be Signed by Client, and Attorney Under Some Circumstances.

8.23 Response Must Be Served on Other Parties.

8.24 Response to Request for Production of ESI (With Table of Common Objections).



100 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court
I. STRATEGY

1-8 MB Practice Guide: CA E-Discovery and Evidence 8.01

8.01 Scope.

This chapter covers the procedure for evaluating and responding to a request for discovery of electronically stored information in California state court, including:

- Developing a response strategy [*see 8.03-8.11*].
- Options for response.
- Preparing and filing a written response to an electronic discovery request [*see 8.12-8.23*].



101 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court

I. STRATEGY

1-8 MB Practice Guide: CA E-Discovery and Evidence 8.02

8.02 Objective and Strategy.

A party to litigation who is served with an e-discovery demand must decide how to respond to that demand. This entails the creation of an e-discovery strategy, which is discussed in 8.03-8.11. Once the strategy has been developed, respondent's counsel must prepare and file a written response to the e-discovery request, as in other types of discovery. In between receipt of the demand and filing a written response, there may be a good deal of informal contact between counsel for the parties, as well as an assessment by the respondent of what and how much ESI exists and how much of the requested ESI has any potential bearing on the litigation.

The actual process of producing ESI in response to a request for production is covered in Ch. 9, Gathering and Producing Electronically Stored Information. The procedure for objecting to demands for production of evidence is discussed in Ch. 10, Opposing Request for Production of Electronic Evidence in California Court. The procedure and grounds for seeking a protective order in response to an e-discovery demand are discussed in Ch 11, Seeking or Opposing Protective Order.



Warning--Attorney Must Understand Ethical Obligations:

There are a number of potential pitfalls in connection with responding to requests for discovery of ESI, and it is important that attorneys review and understand their obligations before undertaking to respond to an e-discovery request. They should also understand the importance of adhering to their ethical obligations in this area, as the penalties for failure to do so can include sanctions, as well as professional discipline in extreme cases.



Cross References:

For a detailed discussion of the process for producing ESI, see Ch. 9, Gathering and Producing Electronically Stored Information.

For discussion of the "meet and confer requirement" and its role in establishing the scope of ESI production, see Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference.

For discussion of ethical obligations in e-discovery, see Ch. 3, Ethical Issues for Attorneys in E-Discovery.

For discussion of sanctions for noncompliance with discovery, see *Ch. 13, Seeking or Opposing Sanctions for Noncompliance, 13.11-13.14*.



102 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court
II. DEVELOPING RESPONSE STRATEGY

1-8 MB Practice Guide: CA E-Discovery and Evidence 8.03

8.03 CHECKLIST: Developing Response Strategy.

☐ Contact client immediately upon receipt of e-discovery request:

☐ Meet with client to formulate a response strategy.

☐ Work with client to understand client's procedures, methods of preservation, and other technical information regarding client's electronic data.

☐ Educate client on legal requirements with respect to e-discovery, importance of compliance, and dangers of noncooperation or failing to take e-discovery process seriously.

☐ Begin immediately upon receipt of an electronic discovery request or upon reasonable anticipation of litigation.

Discussion:

See 8.05

☐ Analyze discovery request.

☐ Determine if ESI exists and is in client's possession.

☐ Instruct client to make a "diligent search and a reasonable inquiry."

☐ If it is discovered that information is in custody or control of someone else, note that information to be conveyed to requesting party.

Authority:
CCP § 2031.230

Discussion:
See 8.06[1]

- ☐ Evaluate whether request is overbroad or unduly burdensome.

Authority:
CCP §§ 2031.210, 2017.010, 2017.020, 2031.060(f)

Discussion:
See 8.06[1]

- ☐ Is all requested ESI relevant to action?
- ☐ Is ESI either admissible in evidence or appears reasonably calculated to lead to discovery of admissible evidence?
- ☐ Does burden, expense, or intrusiveness of requested discovery clearly outweigh likelihood that information sought will lead to discovery of admissible evidence?
- ☐ Can information be obtained from some other source that is more convenient, less burdensome, or less expensive?
- ☐ Is request unreasonably cumulative or duplicative?
- ☐ Does likely burden or expense outweigh likely benefit, taking into account amount in controversy, resources of parties, importance of issues in litigation, and importance of requested discovery in resolving these issues?
- ☐ Assess options for responding to each item or category of request, either:
- ☐ Produce information as requested.

Authority:
CCP §§ 2031.010, 2031.210(1), 2031.060(a)

Discussion:
See 8.07[1]

- ☐ Object to production in whole or in part.

Authority:

CCP §§ 2031.240

Discussion:

See 8.07[2]

- ☐ Seek a protective order.

Authority:

CCP § 2031.060

Discussion:

See 8.07[3]; see also Ch. 11, Seeking or Opposing Protective Order.

- ☐ Assess whether to seek cost shifting or cost sharing.

Authority:

CCP §§ 2031.060, 2031.280(d)

Discussion:

See 8.08

- ☐ Decide form in which ESI will be produced.

- ☐ Form specified in request.

Authority:

CCP § 2031.030(a)(2)

Discussion:

See 8.09[1]

- ☐ Form in which it is maintained in ordinary course of business.

Authority:

CCP § 2031.280(d)(1)

Discussion:

See 8.09[2]

- ☐ Form that is reasonably usable.

Authority:

CCP § 2031.280(d)(1)

Discussion:

See 8.09[3]

- ☐ Address issues of privileged and confidential information.

- ☐ Review ESI for privileged and confidential information.

Authority:

CCP § 2031.285(a); Evid Code § 912(a)

Discussion:

See 8.10

- ☐ Make sure that discovery plan will result in production of responsive ESI in timely manner.

Authority:

CCP §§ 2031.280, 2031.260, 2031.010

Discussion:

See 8.11



103 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court
II. DEVELOPING RESPONSE STRATEGY

1-8 MB Practice Guide: CA E-Discovery and Evidence 8.04

8.04 Options and Strategies.

Through the planning, meet and confer, and case management processes [see discussion in Ch. 4, Planning E-Discovery and Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference], respondent's counsel should have developed a preliminary e-discovery response strategy. Upon receipt of a written e-discovery demand, counsel must review and revise that strategy to the extent necessary, and then begin to implement the strategy. This will typically entail a general review of what is being asked for, and an assessment of whether any materials within the scope of the demand are subject to objection based on relevance, privilege, or other permissible legal bases. Counsel also must decide whether to begin preparing a formal response to the request or to move immediately for a protective order.

In practice, an e-discovery response often involves all of the above components--that is, the respondent typically will agree to provide some requested items, object to providing others, and may move for a protective order as to still others. While these various topics are discussed separately in this publication for more logical organization, in "real world" practice the division is less clear and the response strategy may include both the production of evidence [see Ch. 9, Gathering and Producing Electronically Stored Information], the objection to requested forms of production [see Ch. 10, Gathering and Producing Electronically Stored Information], and seeking a protective order as to other requested ESI [see Ch. 11, Seeking or Opposing Protective Order].

An effective response strategy will do the following:

- Evaluate whether the scope of the request is overbroad or unduly burdensome.
- Identify persons likely to have the information requested.
- Determine and adhere to relevant time frames for responding.
- Determine whether backup data is available and, if not, whether inaccessible data needs to be preserved.
- Determine options for responding.
- Determine whether cost shifting or sharing is available.

- Determine the process for locating, reviewing (for privilege and confidentiality) and producing relevant ESI in a timely manner.

Another important component of the response strategy is negotiation with the opposing party. By the time a demand is filed, it may be expected that counsel will have had their required "meet and confer" meeting as well as a good deal of informal contact. If this is the case, consideration of an appropriate response strategy will begin, in most cases, even before receipt of the demand.

**Cross References:**

For discussion of the production of ESI in connection with an e-discovery response, see Ch. 9, Gathering and Producing Electronically Stored Information.

For discussion of the legal bases and procedures for objecting to the production of ESI in connection with an e-discovery request, see Ch. 10, Gathering and Producing Electronically Stored Information.

For discussion of the grounds and procedures for seeking a protective order, see Ch. 11, Seeking or Opposing Protective Order.

For coverage of an attorney's ethical requirements in connection with e-discovery, see Ch. 3, Ethical Issues for Attorneys in E-Discovery.



104 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court
II. DEVELOPING RESPONSE STRATEGY

1-8 MB Practice Guide: CA E-Discovery and Evidence 8.05

8.05 Responding Party's Counsel Should Contact Client Immediately to Begin Formulating Response Strategy.

Counsel for the responding party should meet with the client to formulate a response strategy as soon as possible upon receipt of an electronic discovery request. To the extent that counsel has not done so earlier in the case, counsel should work with the client to understand the client's procedures, methods of preservation, and other technical information regarding the client's electronic data [see The Sedona Conference, The Sedona Guidelines: Best Practice for Managing Information & Records in the Electronic Age, No. 6].



Strategic Point:

A primary goal for counsel with respect to e-discovery should be ensuring client cooperation and educating the client as to the process. It may be expected that clients are going to be less than enthusiastic about turning over records and documents to an opposing party, and the importance of cooperation and honesty should be emphasized and documented. Counsel should ensure that the client understands the legal requirements with respect to e-discovery, the importance of compliance, and the dangers of failing to take the e-discovery process seriously or failing to cooperate in producing validly requested information.



105 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court
II. DEVELOPING RESPONSE STRATEGY

1-8 MB Practice Guide: CA E-Discovery and Evidence 8.06

8.06 Counsel Should Analyze Request.

8.06[1] Counsel Should Determine If ESI Exists and Is In Client's Possession. A party obviously cannot produce ESI that does not exist or is not in the party's possession. In such a case, the client is required to affirm that a "diligent search and a reasonable inquiry" has been conducted in an effort to comply with the demand [CCP § 2031.230]. If the information in question has never existed, was destroyed, lost, misplaced, or stolen, or was never in the responding party's possession or control, that information must be included in the representation of inability to comply [CCP § 2031.230].

The statement is also required to state the name and address of any natural person or organization known or believed by that party to have possession, custody, or control of an item or category of items of requested ESI [CCP § 2031.230]. The statute is not clear as to how much effort or investigation, if any, is required to determine if ESI is in someone else's possession. However, because the statute requires statements supported by knowledge or belief, if the "diligent search and reasonable inquiry" required by CCP § 2031.230 has uncovered such information, it must be passed along.

➤ **Cross References:**

Drafting response to request for ESI, see 8.12-8.23.

Locating and producing ESI in response to request, see Ch. 9, Gathering and Producing Electronically Stored Information.

8.06[2] Counsel Should Evaluate Whether Request Is Overbroad or Unduly Burdensome. Upon receipt of an electronic discovery request, counsel should review and evaluate the request and assess whether it is too broad, unreasonably cumulative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive. The following issues should be specifically addressed:

- Is all requested ESI relevant to the action [see CCP § 2017.010]?
- Do the requests ask for ESI by "specifically describing each individual item or by reasonably particularizing each category"? [see 2031.030(c)]

- Is the ESI admissible in evidence, or does it appear reasonably calculated to lead to the discovery of admissible evidence [see *CCP* § 2017.020]?
- Does the burden, expense, or intrusiveness of the discovery clearly outweigh the likelihood that the information sought will lead to the discovery of admissible evidence [see *CCP* § 2017.020]?
- Is it possible to obtain the information from some other source that is more convenient, less burdensome, or less expensive [see *CCP* § 2031.060(f)(1)]?
- Is the request unreasonably cumulative or duplicative [see *CCP* § 2031.060(f)(2)]?
- Does the likely burden or expense outweigh the likely benefit, taking into account the amount in controversy, the resources of the parties, the importance of the issues in the litigation, and the importance of the requested discovery in resolving these issues [see *CCP* § 2031.060(f)(4)]?

A request that states "describe and provide any and all documents that pertain to the complaint" is probably overbroad. An objection may be appropriate as to requests that are deemed overbroad or pose an undue burden.

Decision Point:

Although overbroad discovery requests are often criticized as a "fishing expedition," counsel objecting to such requests must do so on the basis that the request does not specifically request sufficient information or that the burden and cost of providing the information is not warranted by the value of the information, and not on the basis of a "fishing expedition" claim [*Irvington-Moore, Inc. v. Superior Court* (1993) 14 CA4th 733, 739, 18 CR2d 49] .

➤ **Cross References:**

Discussion regarding overbroad and overly burdensome ESI, see *Ch. 6, Demanding Production of Electronically Stored Information in California Court*, 6.11.

General coverage of scope of discovery, see *Matthew Bender(R) Practice Guide: California Civil Discovery*, 2.07[4]



106 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court
II. DEVELOPING RESPONSE STRATEGY

1-8 MB Practice Guide: CA E-Discovery and Evidence 8.07

8.07 Counsel Should Assess Options for Responding to Each Item or Category in Request.

8.07[1] Party May Produce Information As Requested. Absent an agreement by the parties, a statement of objection, or a motion for protective order, a party subject to a discovery request is required to produce the information requested. A party may produce the information in the form specified in the request, or in the form in which the ESI is ordinarily maintained, or in a form that will be reasonably useable by the requesting party. Sanctions for failing to produce responsive documents may apply and should be avoided [*CCP* §§ 2031.010, 2031.210(1), 2031.060(a); *Rowe Entm't, Inc. v. William Morris Agency, Inc.* (SDNY 2002) 205 FRD 421, 429 (explaining that even a vast volume of records must be searched in response to a discovery request)].

➡ **Cross References:**

Discussion of properly formatting written response, see 8.16.

Discussion of production of ESI, see Ch. 9, Gathering and Producing Electronically Stored Information.

Discussion of statement of compliance or inability to comply, see 8.19.

8.07[2] Party May Object to Production in Whole or in Part. A responding party may object to an item or category of the discovery request [*CCP* § 2031.240]. The objection must identify the item or category as to which the objection is made and expressly state the reason or grounds for the objection [*CCP* § 2031.240(b)(1)-(2)]. Grounds for objection may be based on relevance, breadth, privilege, undue burden, or confidentiality.

➡ **Cross Reference:**

Detailed discussion of grounds for objection, see Ch. 10, Opposing Request for Production of Electronic Evidence in California Court.

8.07[3] Party May Seek a Protective Order. Instead of simply objecting to a request and awaiting a motion to compel, a responding party may move for a protective order if an agreement cannot be reached between the parties [*CCP* § 2031.060(a)]. In the context of electronic discovery, a frequent rationale for seeking a protective order is that the requested information is not reasonably accessible [*CCP* § 2031.060(b)]. Upon a showing of good cause, the court has broad discretion to grant a protective order, which may include the following provisions [*CCP* § 2031.060(c)]:

- That the discovery not be made.
- That the time of discovery be extended.
- That the discovery be made only on specified terms and conditions, including a designation of the time or place.
- That certain matters not be inquired into, or that the scope of the discovery be limited in some way.
- That the items produced be sealed and thereafter opened only on order of the court.

**Warning:**

A party who unsuccessfully makes or opposes a motion for a protective order is subject to a monetary sanction unless the court finds that the party acted with substantial justification or that other circumstances make the imposition of the sanction unjust [*CCP* § 2017.020(b)].

**Cross Reference:**

See Ch. 11, Seeking or Opposing Protective Order.



107 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court
II. DEVELOPING RESPONSE STRATEGY

1-8 MB Practice Guide: CA E-Discovery and Evidence 8.08

8.08 Cost Shifting or Sharing Can Be Sought.

Generally, the responding party pays for the production of documents, including production of ESI [*Oppenheimer Fund, Inc. v. Sanders* (1978) 437 US 340, 358, 98 S Ct 2380, 57 L Ed2d 253 (in dicta, noting that the federal rules allow shifting of discovery costs from the general rule that the responding party pays); see *San Diego Unified Port Dist. v. Douglas E. Barnhart, Inc.* (2002) 95 CA4th 1400, 1404, 116 CR2d 65 (although responding party usually bears discovery cost, the court lacked authority to order the responding party to share in the cost of destructive testing)].

However, the Electronic Discovery Act allows cost shifting when:

- Translation of ESI into a readable format is required [see CCP §§ 2031.280(e), 1985.8(g) (third-party subpoena); *Toshiba Am. Elec. Components Inc. v. Superior Court* (2004) 124 CA4th 762, 769, 21 CR3d 532 (cost shifting due to translation required by statute)]; or
- The court determines information is not "readily accessible," but the court orders production anyway subject to a condition of cost shifting [see CCP §§ 2031.060(e), 1985.8(e) (cost shifting with respect to third-party subpoena)].

Federal courts have allowed cost shifting when the burden of production outweighs the benefit [*Thompson v. United States Department of Housing and Urban Development* (D Md 2003) 219 FRD 93 (stating that "courts have attempted to fashion reasonable limits that will serve the legitimate needs of the request party for information, without unfair burden or expense to the producing party"; see, e.g. *OpenTV v. Liberate Techs.* (ND Cal 2003) 219 FRD 474, 479 (cost of extraction of source code to be split equally, noting that the substantial time and expense needed to extract data and create data in usable form as factors that earmarked the electronic data as inaccessible)].

In determining whether the cost burden of producing certain data should fall on the requesting or producing party, federal courts have employed several balancing tests. In one seminal case on the topic, the court looked at the following seven factors to determine whether cost shifting should apply [*Zubulake v. UBS Warburg LLC* (SDNY 2003) 217 FRD 309, 324 ; *Rowe Entm't, Inc. v. William Morris Agency, Inc.* (SDNY 2002) 205 FRD 421, 432-433] :

- The extent to which the request is specifically tailored to discovery of relevant information.
- The availability of such information from other sources.

- The total cost of production, compared with the amount in controversy.
- The total cost of production, compared with 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.
- The relative benefits to the parties of obtaining the information.

Examples:

■ Lexar sought production of documents from Toshiba, including "electronic mail" and "other forms of electronically or magnetically maintained information." Toshiba produced 20,000 pages of documents, but a dispute arose when Lexar requested production of additional material from Toshiba's more than 800 computer backup tapes. The cost of processing the backup tapes to obtain potentially relevant information was estimated at between \$1.5 and \$1.9 million, and Toshiba asked Lexar to bear some or all of the cost. Lexar refused and filed a motion to compel production of all responsive documents on the backup tapes. The trial court granted Lexar's motion and did not require Lexar to bear any of the cost. Toshiba requested a stay of the order to produce. The court of appeal felt the issues were "sufficiently novel and important" to justify immediate appellate review, especially given the increasingly frequent discovery requests seeking data from backup tapes. Analyzing the language of former *CCP* § 2031, which provided "[i]f necessary, the responding party at the reasonable expense of the demanding party shall, through detection devices, translate any data compilations included in the demand into reasonably usable form," the court held that cost-shifting was mandatory because translation was required [*Toshiba Am. Elec. Components Inc. v. Superior Court* (2004) 124 CA4th 762, 21 CR3d 532] .

■ Defendant argued that by agreeing to make its complete database available for inspection and copying, it had satisfied its obligations by making the source code available for inspection in the order and manner in which it was kept in the ordinary course of business. The court found that it would take between 125 and 150 hours of work to complete the extraction process for the multiple versions of source code requested by plaintiff and that the requested electronic data was stored in an inaccessible format. Since the requested source code was highly likely to contain relevant information and was unavailable from another source, the court ordered cost-shifting and the responding party was required to bear a portion of the cost of reducing the source code to a usable form [*OpenTV v. Liberate Techs.* (ND Cal 2003) 219 FRD 474] .



Cross References:

Additional discussion of cost shifting in electronic discovery, see *California Forms of Pleading and Practice*, § 190.24 (Matthew Bender).

For additional discussion of the *Zubulake* cost-shifting test, see Matthew Bender(R) Practice Guide: Federal Pretrial Civil Procedure in California, Ch. 23, Methods of Discovery.



108 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court
II. DEVELOPING RESPONSE STRATEGY

1-8 MB Practice Guide: CA E-Discovery and Evidence 8.09

8.09 Respondent Must Decide Form in Which ESI Will Be Produced.

8.09[1] Respondent May Produce ESI in Form Specified in Request. The request for production of electronically stored information may specify the form or forms in which the information is to be produced [CCP § 2031.030(a)(2)]. If the responding party objects to the form specified, or if no form is specified in the request, the responding party must state in its response the form or forms of production it intends to use [CCP § 2031.280(c)]. A party need not produce the same electronically stored information in more than one form [CCP § 2031.280(d)(2)].

 Cross Reference:

Discussion detailing manner of production, see Ch. 9, Gathering and Producing ESI.

8.09[2] Respondent May Produce ESI in Form in Which It Is Maintained in Ordinary Course of Business. If the form in which the electronically stored information is to be produced is not specified in the request, or unless the parties otherwise agree or the court otherwise orders, the information may be provided in a form in which it is ordinarily maintained or in a form that is reasonably usable [CCP § 2031.280(d)(1)]. Courts will look at how the respondent keeps electronic records in the ordinary course of business in order to determine the appropriateness of the format in which the information is sought or delivered.

8.09[3] Respondent May Produce ESI in a Form That Is Reasonably Usable. If the form in which the electronically stored information is to be provided is not specified in the request, the information may be provided in a form that is "reasonably usable" by the requesting party [CCP § 2031.280(d)(1)].

 Cross Reference:

For discussion of "native" format vs. "reasonably useable," see Ch. 6, *Demanding Production of Electronically Stored Information in California Court*, 6.07.

**Strategic Point--Producing Party--Organization of Documents:**

Whether the producing party decides to produce ESI in native format (e.g., "in the form or forms in which it is ordinarily maintained") or in another "form that is reasonably usable" [see CCP § 2031.280(d)(1)], the party should still be mindful of the requirement to organize the produced ESI

pursuant to the requirements of *CCP § 2031.280(a)*.

CCP § 2031.280(a) gives the producing party the choice of either organizing the documents by document request number, or producing them "as they are kept in the usual course of business," that is, grouped together in the same manner and with the same relationships in which they are kept in the producing party's files or storage systems. When paper originals were collected in the past, this meant that a party who collected responsive documents from 10 different witnesses could produce all of the papers from a particular person together instead of having to rearrange the documents in the production so that documents from all 10 witnesses that were responsive to a particular document request were in the same pile. The "as they are kept in the usual course of business" alternative eliminated the need to identify the document request to which each particular paper document was responsive.

Analogously, with respect to ESI, the responding party need not issue-tag each particular item of ESI with the corresponding document request. However, the ESI should be produced in a manner that preserves information about the original relationships between items of ESI in the producing party's storage systems. For example, if a party is producing TIFF images of e-mails that have Word document attachments, the load file should provide information that clearly identifies to which e-mail a particular Word document was attached, and which custodian's in-box, out-box or trash it came from. If native files are produced, they should be organized with the same directory structure of folders and subfolders as on the server or computer from which they came. The best practice is to agree with opposing counsel, in advance of production, what information will be included in the load files. Such agreements will help avoid discovery disputes on these issues.



109 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court
II. DEVELOPING RESPONSE STRATEGY

1-8 MB Practice Guide: CA E-Discovery and Evidence 8.10

8.10 Respondent Should Address Issues of Privileged and Confidential Information.

8.10[1] Counsel Should Review ESI for Privileged and Confidential Information. It is vitally important that a party review any responsive documents for privileged or confidential information to avoid risking attorney-client privilege waivers and other adverse consequences of inadvertent production.

Electronic evidence is especially vulnerable to inadvertent disclosure of privileged or confidential information because of how electronic information is stored, maintained, updated and changed. As such, counsel should employ a sound review practice for sifting out privileged or confidential information including, but not limited to, the use of computer software designed specifically to analyze e-mails (including "metadata") and other electronic documents by converting them into a more easily reviewable and field-searchable form. A sound review process will not only help minimize inadvertent production, but also will help lay a foundation to excuse any waiver the opposing party might argue for in court based on the party's exercise of reasonable efforts to avoid inadvertent production.

Example:

■ Attorneys for plaintiff produced a CD-ROM of e-mails without reviewing the e-mails. As a result, 227 attorney-client privileged e-mails (or four percent of the entire document production) were produced as part of a large electronic production that encompassed five thousand e-mail files. Plaintiff's counsel had not sought a claw-back agreement. The court determined that, "on balance, and using a holistic reasonableness analysis, the court finds that plaintiff Infor has waived the privilege" [*Infor Global Solutions (Michigan), Inc. v. St. Paul Fire & Marine Ins. Co. (ND CA Aug 3, 2009) 2009 U.S. Dist. LEXIS 71370, *3-*8*] .

■ In *Victor Stanley, Inc. v. Creative Pipe, Inc. (D Md 2008) 250 FRD 251* , the court found that the attorney-client privilege had been waived for inadvertently produced documents when the electronic search process for identifying privileged documents was not reasonable.

Strategic Point:



Issues related to privileged and confidential matters are best handled early in the case during discovery planning meetings and meet and confer conferences. Counsel should agree precisely how all forms of privileged and confidential documents will be dealt with in discovery [*Cal Rules Ct, Rule 3.724; CCP § 2018.030*].

Cross References:

Discussion of initial procedures in e-discovery and meeting and conferring, see *Chapter 4, 4.03-4.10, Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferring, and Case Management, 5.14-5.21*.

8.10[2] Inadvertent Disclosure of Privileged Information May Result in Waiver of Privilege. Generally, a party who discloses part or all of privileged information to another party waives its right to a claim of privilege to the information [*Evid Code § 912(a)*].

Exception:

The producing party may take back inadvertently produced ESI if it notifies the receiving party of a claim that ESI that was produced in discovery is privileged or protected as attorney work product (this is known as the "clawback" provision) [*CCP § 2031.285(a)*].

Cross Reference:

Detailed discussion of clawback rule, see *Ch. 3, Ethical Issues for Attorneys in E-Discovery, 3.14*.

8.10[3] Producing Party Must Immediately Notify the Receiving Party of Any Inadvertent Disclosure of Privileged Information. A party making a claim that electronically stored information inadvertently produced in discovery is privileged or protected as attorney work product should notify the receiving party of the claim that the information is privileged or protected [*CCP § 2031.285(a)*].

8.10[4] Receiving Party Must Promptly Return to Sender Privileged Information. After being notified of a claim of privilege or protection as attorney work product, the receiving party must promptly sequester the information and either return the information (and any copies), or present the information to the court conditionally under seal for a determination of the claim. Until resolution, the receiving party is required to preserve the information and keep it confidential [*CCP § 2031.285(b)*; *Rico v. Mitsubishi Motors Corp. (2007) 42 C4th 807, 817, 68 CR3d 758, 171 P3d 1092*].



Timing:

The receiving party has 30 days after receipt of privileged or protected information to move the court to address the validity of the privilege claim or it will lose the ability to use that document. Until the claim is resolved, the receiving party must preserve the information and keep it confidential [*CCP § 2031.285*].



Warning:

A party who fails to notify the opposing counsel that it has received privileged information and makes full use of the privileged documents may be disqualified. In *Rico v. Mitsubishi Motors Corp.*, plaintiff's attorney received inadvertently produced notes of a discussion between opposing counsel and their expert witness. Although the document was not labeled as attorney work product, the court held that it was "absolutely privileged" by the attorney work product rule. Upon finding the document, the plaintiff's attorney not only failed to notify defendant's counsel, but gave copies of the document to co-counsel and the plaintiff's expert witness, and used the document in deposing the defendant's expert. The court found that the plaintiff's attorney acted unethically by failing to notify defendant and instead "surreptitiously using it to gain maximum adversarial value from it" [*Rico v. Mitsubishi Motors Corp. (2007) 42 C4th*

807, 813, 68 CR3d 758, 171 P3d 1092] .



Cross Reference:

Discussion of ethical issues for attorneys in e-discovery, see Chapter 3, Ethical Issues for Attorneys in E-Discovery.



110 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court
II. DEVELOPING RESPONSE STRATEGY

1-8 MB Practice Guide: CA E-Discovery and Evidence 8.11

8.11 Responsive Documents Must Be Produced in Timely Manner.

After serving a written response stating a party's intention to comply or object, the responding party must produce responsive ESI in a timely manner. The ESI may be produced in various forms of production, depending on the form requested in the initial discovery request or as identified in the response letter stating the form in which the responding party intends to produce. The responding party should produce responsive ESI by conforming to the time and manner of compliance as agreed upon [CCP §§ 2031.280, 2031.260, 2031.010].



Cross Reference:

See Ch. 9, Gathering and Producing ESI.



111 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court
III. PREPARING WRITTEN RESPONSE TO ELECTRONIC DISCOVERY REQUEST

1-8 MB Practice Guide: CA E-Discovery and Evidence 8.12

8.12 CHECKLIST: Preparing Written Response to Electronic Discovery Request.

☐ Review applicable time requirements and plan to make a timely response to discovery request, either:

☐ Within 30 days after receiving discovery request; or

Authority:
CCP § 2031.260(a)

Discussion:
See 8.14

☐ Enter into written agreement with opposing parties to shorten or lengthen response period.

Authority:
CCP § 2031.270

Discussion:
See 8.14

☐ Draft written response.

☐ Immediately below title of case, include identity of responding party, set number, and identity of demanding party.

Authority:
CCP § 2031.210(b)

Discussion:

See 8.16

- ☐ Respond to each item or category in demand.

Authority:

CCP § 2031.210

Discussion:

See 8.17

☐ Each response must be clearly identified, bear same number, and be in same sequence as corresponding item or category in demand.

Authority:

CCP § 2031.210(c)

Discussion:

See 8.18

- ☐ Response should state one of following as to each item or category of item:

☐ That party will comply, in whole or part, with the particular demand for inspection and any related activities.

☐ That party lacks the ability to comply with demand for inspection or a particular item or category of item.

☐ An objection to the particular demand.

Authority:

CCP § 2031.210

Discussion:

See 8.17

- ☐ Statement of compliance must include statement that:

☐ Production, inspection, and any related activity demanded will be allowed either in whole or in part; and

☐ All documents or things in demanded category that are in possession, custody, or control of that party (if no objection is being made) will be included in production.

Authority:

CCP § 2031.220

Discussion:*See 8.19[1]*

- ☐ Representation of inability to comply with a particular demand must:
- ☐ Affirm that diligent search and reasonable inquiry has been made in order to comply with demand for production.
 - ☐ Specify whether inability to comply is because particular item or category has never existed, has been destroyed, has been lost, misplaced, or stolen, or has never been, or is no longer, in possession, custody, or control of responding party [CCP § 2031.230].
 - ☐ Include name and address of any natural person or organization known or believed by that party to have possession, custody, or control of that item or category of item [CCP § 2031.230].

Authority:*CCP § 2031.230***Discussion:***See 8.19[2]*

- ☐ Specify form of production respondent intends to use if:
- ☐ Request did not state a form, or
 - ☐ Responding party objects to form specified in request.

Authority:*CCP § 2031.280(c)***Discussion:***See 8.20*

- ☐ State any applicable objections for each item, category of item, or part of an item or category, for which responding party has not indicated a willingness to comply or has not represented an inability to comply.
- ☐ Identify with particularity any ESI falling within any category of item to which an objection is being made; and
 - ☐ Set forth clearly extent of and specific ground for objection.
 - ☐ If objection is based on a privilege claim, particular privilege invoked must be expressly asserted.

☐ If objection is based on claim that information sought is protected work product, that claim must be expressly stated.

Authority:

CCP § 2031.240(b)

Discussion:

See 8.21

☐ Have response signed by:

☐ Client under oath, unless response contains only objections.

☐ Attorney, if response contains any objections.

Authority:

CCP § 2031.250(b), (c)

Discussion:

See 8.22

☐ Serve response.

☐ Serve original on party that made the demand.

☐ Serve copies on all other parties to action.

☐ Serve response within 30 days after service of demand unless:

☐ On motion of party making demand, court has shortened time for response, or

☐ On motion of party to whom demand has been directed, court has extended time for response.

☐ Special rules apply in unlawful detainer actions.

Authority:

CCP § 2031.260

Discussion:

See 8.23

☐ Do not file response with court.

Authority:

CCP § 2031.290(a)

Discussion:

See 8.23



112 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court
III. PREPARING WRITTEN RESPONSE TO ELECTRONIC DISCOVERY REQUEST

1-8 MB Practice Guide: CA E-Discovery and Evidence 8.13

8.13 Options and Strategy.

In drafting a response to a request for production of ESI, counsel's goals should be both to comply with statutory requirements governing content and completeness, and to assert and preserve any objections that the respondent may be entitled to claim with respect to the demand. Thus, the overall response should be thorough and complete, and the individual responses articulated in sufficient detail to clearly state the basis for each response. The response should be filed in conformity with all applicable time requirements.



113 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court
III. PREPARING WRITTEN RESPONSE TO ELECTRONIC DISCOVERY REQUEST

1-8 MB Practice Guide: CA E-Discovery and Evidence 8.14

8.14 Making a Timely Response to Electronic Discovery and Inspection Request.

The party upon whom a request for production of documents and things, including electronically stored information, is served must serve a written response within 30 days after the service of the request. The original response should be served on the party making the demand whereby a copy of the response should be served on all other parties who have appeared in the action [CCP § 2031.260(a)].

Parties may make agreements to shorten or lengthen the time for response to an electronic discovery demand pertaining to a set or to particular items or categories of items in a set [CCP § 2031.270(a)]. To be effective, the agreement must be in writing and specify the extended date for inspection or service of a response [CCP § 2031.270(b)].



Strategic Point--Negotiate Additional Response Time:

Extensions of time for response are frequently necessary due to the large volumes of ESI that must often be reviewed to respond. If possible, such agreements for adequate time to respond to discovery should be negotiated in early meet and confer discussions [see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management, 5.14-5.21*].



114 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court
III. PREPARING WRITTEN RESPONSE TO ELECTRONIC DISCOVERY REQUEST

1-8 MB Practice Guide: CA E-Discovery and Evidence 8.15

8.15 Failure to Serve Timely Response May Result in Monetary and Other Sanctions.

Generally, a failure to respond to discovery requests within the time required constitutes a waiver of any objections, including an objection based on privilege or work product protection [*CCP* § 2031.300(a)]. However, a court may determine that a party's failure to make a timely response does not amount to waiver if the party has subsequently served a response that is in substantial compliance with discovery response obligations and the failure was a result of mistake, inadvertence, or excusable neglect [*CCP* § 2031.300(a)(1)(2)].



Cross Reference:

Detailed discussion of sanctions, see Ch. 13, Seeking or Opposing Sanctions for Noncompliance.



115 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court
III. PREPARING WRITTEN RESPONSE TO ELECTRONIC DISCOVERY REQUEST

1-8 MB Practice Guide: CA E-Discovery and Evidence 8.16

8.16 Response Must Be Properly Formatted.

The first paragraph of the response immediately below the title of the case should include the identity of the responding party, the set number, and the identity of the demanding party [*CCP* § 2031.210(b)].



116 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court
III. PREPARING WRITTEN RESPONSE TO ELECTRONIC DISCOVERY REQUEST

1-8 MB Practice Guide: CA E-Discovery and Evidence 8.17

8.17 Response Must Address Each Item or Category in Demand.

The responding party must respond to each item or category of item. The response must contain any of the following [CCP § 2031.210]:

- A statement that the party will comply, in whole or part, with the particular demand for inspection and any related activities [see 8.19[1], 8.20];
- A representation that the party lacks the ability to comply with the demand for inspection of a particular item or category of item [see 8.19[2]]; or
- An objection to the particular demand [see 8.21].



117 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court
III. PREPARING WRITTEN RESPONSE TO ELECTRONIC DISCOVERY REQUEST

1-8 MB Practice Guide: CA E-Discovery and Evidence 8.18

8.18 Responses Must Be Clearly Identified.

The response to the inspection or production demand must be clearly identified. Each statement of compliance, representation, and objection must bear the same number and be in the same sequence as the corresponding item or category in the demand [CCP § 2031.210(c)].



Strategic Point:

Although the text of a request is not required to be repeated in the responses, it is common practice to do so. Repeating the requests is recommended as it makes the responses easier to understand and review.



118 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court
III. PREPARING WRITTEN RESPONSE TO ELECTRONIC DISCOVERY REQUEST

1-8 MB Practice Guide: CA E-Discovery and Evidence 8.19

8.19 Response Must Include Statement of Compliance or Inability to Comply.

8.19[1] Contents of Statement of Compliance. A statement that the party will comply with the demand [see CCP § 3031.210(a)(1); 8.17] must state the following [CCP § 2031.220]:

- That the production, inspection, and any related activity demanded will be allowed either in whole or in part; and
- That all documents or things in the demanded category that are in the possession, custody, or control of that party (where no objection is being made) will be included in the production.

8.19[2] Contents of Statement of Noncompliance. A representation of inability to comply the particular demand [see CCP § 3031.210(a)(2); 8.17] must affirm that a diligent search and a reasonable inquiry has been made in order to comply with a demand for production of documents and things, including electronically stored documents [CCP § 2031.230].

Cross Reference:

Discussion of what constitutes a "diligent search and reasonable inquiry" with respect to ESI, see 8.06.

The statement must also specify whether the inability to comply is because the particular item or category has never existed, has been destroyed, has been lost, misplaced, or stolen, or has never been, or is no longer, in the possession, custody, or control of the responding party [CCP § 2031.230].

The statement also must include the name and address of any natural person or organization known or believed by that party to have possession, custody, or control of that item or category of item [CCP § 2031.230].

Cross Reference:

Form, see 8.24



119 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court
III. PREPARING WRITTEN RESPONSE TO ELECTRONIC DISCOVERY REQUEST

1-8 MB Practice Guide: CA E-Discovery and Evidence 8.20

8.20 Response Must State Form of Production.

The responding party must state the form of production it intends to use for producing ESI if the request did not state a form or if the responding party objects to the form specified in the request [*CCP* § 2031.280(c)].

Cross References:

Discussion of manner of compliance of inspection or production request, including time and place, see Ch. 9, Gathering and Producing Electronically Stored Information.

Discussion of detailed manner, format, and content of inspection demand, see *California Deposition and Discovery Practice*, Section 61.20.

Form, see 8.24.



120 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court
 III. PREPARING WRITTEN RESPONSE TO ELECTRONIC DISCOVERY REQUEST

*1-8 MB Practice Guide: CA E-Discovery and Evidence 8.21***8.21 Any Applicable Objections to Request for Production of ESI Should Be Stated.**

For each item, category of item, or part of an item or category, for which the responding party has not indicated a willingness to comply or has not represented an inability to comply, the response must state an objection to compliance. Objections to a demand for inspection of an item or category of item in the demand must [CCP § 2031.240(b)]:

- Identify with particularity any ESI falling within any category of item to which an objection is being made; and
- Set forth clearly the extent of, and the specific ground for, the objection.

Strategic Point:

Although the statutory language requires that ESI falling within the objection be identified "with particularity," this is often very difficult to do within the 30-day period after service of an inspection demand within which the response must be filed [see CCP § 2031.260(a)]. In practice, parties often file general categorical objections, particularly as to privilege or work product, to ensure that objections are preserved and not waived. Unlike federal practice, general "boilerplate" objections are sufficient to preserve privilege until the existence of a privilege is challenged [Best Products, Inc. v. Superior Ct. (2004) 119 CA4th 1181, 1188, 15 CR3d 154] . If the existence of the privilege is challenged, the party asserting the privilege then must support the existence of the privilege with a privilege log that identifies the documents or ESI with particularity and provides the factual basis for assertion of the privilege [Best Products v. Superior Ct. (2004) 119 CA4th 1181, 1188, 15 CR3d 154] . Note, in contrast, that in federal courts, such "blanket objections" have been characterized as improper and ineffective [Eureka Fin. Corp. v. Hartford Accident & Indem. Co. (ED Cal 1991) 136 FRD 179, 183-185 ("[a]lthough it may be time-consuming to specifically assert the attorney-client or work product privilege in a document intensive litigation, the courts nevertheless clearly require such specific identification. ... [i]f the privilege is worth protecting, a litigant must be prepared to expend some time to justify the assertion of the privilege")], and several federal courts have held that a non-specific objection by itself serves as a waiver of the privilege asserted [Eureka Fin. Corp. v. Hartford Accident & Indem. Co. (ED Cal 1991) 136 FRD 179, 183 ; see, e.g., Peat, Marwick, Mitchell & Co. v. West (10th Cir. 1984) 748 F2d 540, 541-542] .

If the objection is based on a privilege claim, the particular privilege invoked (such as the attorney-client privilege)

must be expressly asserted [*CCP* § 2031.240(b)(2)].

Consider--Claims of Attorney-Client Privilege Belong to Client:

Claims of attorney-client privilege belong to the client (as opposed to claims of attorney work product privilege, which belong to the attorney). Therefore, if the client is a corporation, it must be in good standing to successfully assert claim of attorney-client privilege in a discovery response [see *Software Rights Archive, LLC v. Google Inc.* (ND CA February 2010) 2010 U.S. Dist. LEXIS 11581 ("a dissolved or non-functioning corporation may not assert the attorney-client privilege")].

If the objection is based on the claim that the information sought is protected work product [see *CCP* § 2018.010], that claim must be expressly stated [*CCP* § 2031.240(b)(2)].

Other grounds for objection may include:

- Relevance.
- Trade secret.
- Privacy [see 8.10].
- Undue burden or expense [see *CCP* § 2017.020(a)]; see also 8.06[2]].



Cross Reference:

Detailed discussion of grounds for objections to inspection and production requests, see Ch. 10, Opposing Request for Production of Electronic Evidence in California Court.



121 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court
III. PREPARING WRITTEN RESPONSE TO ELECTRONIC DISCOVERY REQUEST

1-8 MB Practice Guide: CA E-Discovery and Evidence 8.22

8.22 Response Must Be Signed by Client, and Attorney Under Some Circumstances.

The party to whom the demand is directed must sign the response under oath, unless the response contains only objections [CCP § 2031.250(a)]. If the responding party is a public or private corporation, or a partnership or association, or governmental agency, one of its officers or agents must sign the response under oath on the party's behalf [CCP § 2031.250(b)].

The responding party's attorney must sign any response that contains an objection [CCP § 2031.250(c)].



Trap:

If the officer or agent signing the response on behalf of the a party is the responding party's attorney, the party waives any lawyer-client privilege and work product protection during subsequent discovery from that attorney concerning the identity of the sources of the information in the response [CCP § 2031.250(b)].



122 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court
III. PREPARING WRITTEN RESPONSE TO ELECTRONIC DISCOVERY REQUEST

1-8 MB Practice Guide: CA E-Discovery and Evidence 8.23

8.23 Response Must Be Served on Other Parties.

The party to whom the demand is directed must serve the original of the response on the party making the demand, and copies of the response on all other parties to the action [*CCP* § 2031.260(a)]. The response should not be filed with the court [*CCP* § 2031.290(a)]. A proof of service should accompany the responses in case any dispute about proper service later arises.



Timing:

The response must be served with 30 days after service of an inspection demand, unless on motion of the party making the demand the court has shortened the time for response, or unless on motion of the party to whom the demand has been directed the court has extended the time for response [*CCP* § 2031.260(a)]. Special rules apply in unlawful detainer actions [*CCP* § 2031.260(b)].

The party demanding discovery is required to retain the original demand, proof of service, and response until six months prior to the final disposition, at which point they may be destroyed unless the court orders otherwise [*CCP* § 2031.290(b)].



123 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 8 Responding to Electronic Discovery Demands in California Court
IV. FORMS*1-8 MB Practice Guide: CA E-Discovery and Evidence 8.24***8.24 Response to Request for Production of ESI (With Table of Common Objections).**

Response to Request for Production of ESI (With Table of Common Objections).

Jane Lee

California Bar Number 123456

50 South Main St., Suite 100

Farallon City, California 90000

Phone: 555-999-9999

Attorney for Defendant, Mary Jones Enterprises, Inc.

SUPERIOR COURT OF CALIFORNIA,

COUNTY OF FARALLON

	)	
	)	No. _____
John Smith, Plaintiff, vs. Mary Jones Enterprises,	)	RESPONSE OF DEFENDANT _____ [e.g.,
Inc., Defendant.	)	MARY JONES ENTERPRISES] TO
	)	_____ [e.g., PLAINTIFF JOHN
	)	SMITH'S]
		FIRST SET OF REQUESTS FOR PRODUCTION
		OF DOCUMENTS

PROPOUNDING PARTY: Plaintiff, John Smith**RESPONDING PARTY:** Defendant, Mary Jones Enterprises, Inc.**SET NO.:** One**PRELIMINARY STATEMENT**

Defendant Mary Jones Enterprises ("Defendant") has not completed its investigation or discovery in this action. All responses to the following requests and any documents identified in those responses by Defendant herein are based upon the information disclosed during preliminary investigations as of the date of these responses. In the event that

Defendant discovers or becomes aware of other information or documents, after further investigation or discovery, it reserves the right to use such information and documents in prosecution of this action. By this reservation, however, Defendant does not assume any continuing responsibility to update its responses that would exceed the requirements of the California Code of Civil Procedure.

[NOTE: The table at the end of this form contains sample responses that illustrate common objections and responses to individual production demands for ESI. Those objections may be inserted into response documents such as this form to raise appropriate objections to specific items or categories of information (see CCP §§ 2031.210--2031.240). In practice it is common to state multiple grounds for objections to individual requests, and to combine objections with statements of compliance. The examples below illustrate how multiple objections are commonly set out in response to particular demands.]

REQUEST FOR PRODUCTION NO. 1:

[Restate request as it appears in demand, e.g. All COMMUNICATIONS between Defendant, Mary Jones Enterprises, Inc. and PLAINTIFF regarding the PREMISES, WORK or AGREEMENT.]

RESPONSE TO REQUEST FOR PRODUCTION NO. 1:

[Objection combining relevance, work product, and privilege objections from table at end of this form, CCP § 2017.010]. Defendant objects to this request on the ground that the requested information is not relevant to the subject matter involved in the pending action or the determination of any motion made in that action. Defendant further objects to this request to the extent that it seeks information or documents that are protected work product under California Code of Civil Procedure Section 2018.010 et seq. and/or protected by the attorney-client privilege and are not subject to discovery.

REQUEST FOR PRODUCTION NO. 2:

[Restate request as it appears in demand]

RESPONSE TO REQUEST FOR PRODUCTION NO. 2:

*[Objection that request is unlikely to produce admissible evidence under CCP § 2017.010, privilege, and work product objections with agreement to partially produce CCP §§ 2031.210(a)(1), 2031.220]. Defendant objects to this request on the ground that the information requested is neither itself admissible into evidence nor appears reasonably calculated to lead to the discovery of admissible evidence. Defendant further objects to this request to the extent that it seeks information or documents that are protected work product under California Code of Civil Procedure Section 2018.010 et seq. and/or protected by the attorney-client privilege and are not subject to discovery. Without waiver of the foregoing objections, Defendant will produce _____ *[describe what will be produced]* that are in the possession, custody, or control of Defendant.*

REQUEST FOR PRODUCTION NO. 3:

[Restate request as it appears in demand]

RESPONSE TO REQUEST FOR PRODUCTION NO. 3:

[Statement of full compliance, *CCP §§ 2031.210(a)(1), 2031.220*] Defendant will comply with this demand by the date set pursuant to *Code of Civil Procedure Section 2031.030(c)(2)(c)*, and all documents or things in the demanded category that are in the possession, custody, or control of Defendant will be included in the production.

REQUEST FOR PRODUCTION NO. 4:

[*Restate request as it appears in demand*]

RESPONSE TO REQUEST FOR PRODUCTION NO. 4:

[Statement of inability to comply, *CCP §§ 2031.210(a)(2), 201.230*] Defendant has made a diligent search and a reasonable inquiry in an effort to comply with this demand, but is unable to comply with this demand because the requested information _____ [*state one or more of the following reasons: never existed or has been destroyed or has been lost, misplaced, or stolen or* _____ (*has never been or is no longer*) in the possession, custody, or control of _____ (*responding party*)]. [Defendant believes that this information is in the possession, custody, or control of _____ (*name of person or organization*), _____ (*address*).]

REQUEST FOR PRODUCTION NO. 5:

[*Restate request as it appears in demand*]

RESPONSE TO REQUEST FOR PRODUCTION NO. 5:

[Statement of partial compliance with inability to comply, *CCP §§ 2031.210(a)(2), 2031.220*] Defendant will comply in part with this demand by the date set pursuant to *Code of Civil Procedure Section 2031.030(c)(2)(c)*, and all documents or things in the demanded category that are in the possession, custody, or control of Defendant will be included in the production. With respect to the remainder of that category, Defendant has made a diligent search and a reasonable inquiry in an effort to comply with this demand, but is unable to further comply with this demand because the requested information _____ [*state one or more of the following reasons: never existed or has been destroyed or has been lost, misplaced, or stolen or* _____ (*has never been or is no longer*) in the possession, custody, or control of _____ (*responding party*)]. [Defendant believes that this information is in the possession, custody, or control of _____ (*name of person or organization*), _____ (*address*).]

FORM OF PRODUCTION

Unless otherwise specified in this response, all documents and other data provided by Defendant in response to Plaintiff's request will be provided in _____ [*specify, e.g., TIFF*] format.

Verification

[Must be signed by responding party under oath unless response contains only objections]

I, Mary Jones, declare:

I am the CEO of MARY JONES ENTERPRISES, INC., a corporation organized and existing under the laws of California. I have been authorized to make this verification on behalf of Mary Jones Enterprises, Inc.

I have read the foregoing RESPONSE OF MARY JONES ENTERPRISES, INC. TO PLAINTIFF JOHN SMITH'S FIRST SET OF REQUESTS FOR THE PRODUCTION OF DOCUMENTS and know the contents thereof. The same is true of my own knowledge, information and belief.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed at _____, California on _____ [date]
 _____ [signature]

Mary Jones

[If response contains any objections, attorney for responding party must sign]

I, Jane Lee, am the attorney for Defendant MARY JONES ENTERPRISES, INC., and have signed this declaration as required by *Code of Civil Procedure Section 2031.250(c)*.

Executed at _____, California on _____ [date]
 _____ [signature]

Table of Common Objections

[The following table identifies responses that illustrate common objections and responses to individual production requests for ESI. The listed objections are not comprehensive; other grounds may also exist for objecting to particular production requests. In addition, in practice it is common to state multiple grounds for objections to individual requests, and to combine objections with statements of compliance. For more detailed discussion of the listed grounds for the production of ESI, see Ch. 10, Opposing Request for Production of Electronic Evidence in California Court.]

[Reason for objection]

[Statement of objection]

[Work product objection, CCP §§ 2031.240(b)(2), 2018.010 et seq.]

Defendant objects to this request on the ground that the information sought is protected work product under California Code of Civil Procedure Section 2018.010 et seq.

[Privilege objection]

Defendant objects to this request on the ground that the information sought is protected by the _____ *[specify privilege, e.g., attorney-client]* privilege and is not subject to discovery.

[Relevance objection, CCP § 2017.010]

Defendant objects to this request on the ground that the requested information is not relevant to the subject matter involved in the pending action or the determination of any motion made in that action.

[Objection that request is unlikely to produce admissible evidence under CCP § 2017.010]

Defendant objects to this request on the ground that the information requested is neither itself admissible into evidence nor appears reasonably calculated to lead to the

	discovery of admissible evidence.
[<i>Undue burden and expense</i> , CCP § 2017.020(a)]	Defendant objects to this request on the ground that the burden, expense, and intrusiveness of the requested discovery clearly outweighs the likelihood that the information sought will lead to the discovery of admissible evidence.
[<i>Objection that benefits outweigh burden</i> , CCP § 231.060(f)(4)]	Defendant objects to this request on the ground that the likely burden or expense of the proposed discovery outweighs the likely benefit, taking into account the amount in controversy, the resources of the parties, the importance of the issues in the litigation, and the importance of the requested discovery in resolving the issues.
[<i>Less burdensome way exists to obtain information</i> , CCP § 231.060(f)(1)]	Defendant objects to this request on the ground that it is possible for plaintiff to obtain the requested information from some other source that is more convenient, less burdensome, or less expensive, specifically _____ [specify].
[<i>Objection that ample opportunity existed</i> , CCP § 231.060(f)(3)]	Defendant objects to this request on the ground that Plaintiff has had ample opportunity by discovery in the action to obtain the information sought.
[<i>Objection that information requested is not reasonably accessible because of undue burden or expense</i> ; CCP §§ 2031.060(c), 2031.210(d)]	Defendant objects to this request on the ground that the information requested is from a source that is not reasonably accessible because of undue burden or expense, specifically _____ [identify types or categories of sources of ESI that are not reasonably accessible, e.g., backup tapes in excess of five years old that were originally prepared using software that is now obsolete and would require hundreds of hours of work to identify and decode, at a cost estimated to be in excess of \$200,000].
[<i>Objection that information is unnecessarily cumulative or duplicative under CCP § 231.060(f)</i>]	Defendant objects to this request on the ground that the discovery sought is unreasonably cumulative or duplicative, in that _____ [specify, e.g., all the information requested in this request will be provided to Plaintiff in printed form under the response to Request for Production No. _____ and an additional production of the identical information in the format requested here is unnecessary].
[<i>Statement of full compliance</i> , CCP §§ 2031.210.a)(1), 2031.220]	Defendant will comply with this demand by [either the date set pursuant to Code of Civil Procedure Section 2031.030(c)(2)(c) or an agreed upon date], and all documents or things in the demanded category that are in the possession, custody, or control of Defendant will be included in the production.
[<i>Statement of partial compliance with objection</i> , CCP §§ 2031.210.a)(1), 2031.220]	Defendant objects to this request on the grounds that _____ [specify objection, see above]. Without waiver of the foregoing objections, Defendant

[Statement of inability to comply, CCP §§ 2031.210.a)(2), 201.230]

will produce [*describe what will be produced*] that are in the possession, custody, or control of Defendant.

Defendant has made a diligent search and a reasonable inquiry in an effort to comply with this demand, but is unable to comply with this demand because the requested information _____ [*state one or more of the following reasons: never existed or has been destroyed or has been lost, misplaced, or stolen or* _____ (*has never been or is no longer*) in the possession, custody, or control of _____ (*responding party*)].

[_____ believes that this information is in the possession, custody, or control of _____ (*name of person or organization*), _____ (*address*).]

[Statement of partial compliance with inability to comply, CCP §§ 2031.210.a)(2), 2031.220]

Defendant will comply in part with this demand by the date set pursuant to Code of Civil Procedure Section 2031.030(c)(2)(c), and all documents or things in the demanded category that are in the possession, custody, or control of Defendant will be included in the production. With respect to the remainder of that category, Defendant has made a diligent search and a reasonable inquiry in an effort to comply with this demand, but is unable to further comply with this demand because the requested information _____ [*state one or more of the following reasons: never existed or has been destroyed or has been lost, misplaced, or stolen or* _____ (*has never been or is no longer*) in the possession, custody, or control of _____ (*responding party*)].

[_____ believes that this information is in the possession, custody, or control of _____ (*name of person or organization*), _____ (*address*).]

NOTES:

Authority:

CCP §§ 2031.210--2031.250

Timing of Response:

See 8.14, 8.15

Contents of Response:

See 8.16-8.21

Objections:

See 8.21; see Ch. 10, Opposing Request for Production of Electronic Evidence in California Court

Signature Requirements:

See 8.22

Serving Response:

See 8.23



124 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.syn

AUTHOR: Ernst Halperin

§ 9.syn Synopsis to Chapter 9: Gathering and Producing Electronically Stored Information

9.01 Scope.

9.02 Objective and Strategy.

9.03 CHECKLIST: Understanding the Case.

9.04 Options and Strategy.

9.05 Civil Discovery Act Defines Parameters of Allowable Discovery.

9.06 Counsel Should Review Pleadings and Motion Papers That Frame the Issues.

9.06[1] Complaint Tells Plaintiffs' Story.

9.06[2] Answer Contains Defendants' Affirmative Defenses.

9.06[3] Papers in Support of and Opposition to Demurrers Often Describe Parties' Themes.

9.06[4] CACI and BAJI Model Jury Instructions List Elements of Each Cause of Action and Affirmative Defense.

9.06[5] Theory of Each Party's Case Provides Useful Information.

9.06[6] Counsel Should Brainstorm Regarding Potential Causes of Action That Were Not Pleaded but Might Be Included in an Amended Complaint and Affirmative Defenses.

9.07 CHECKLIST: Preparing to Gather ESI in Response to a Demand for Production.

9.08 Options and Strategy.

9.09 Counsel Should Consider Whether Engaging an ESI Consultant Would Be Appropriate.

9.10 Counsel Should Meet With Client's In-House Counsel, IT Personnel, and ESI Consultant to Develop Data Collection Plan and Update Data Preservation Plan.

9.11 Understanding Client's Data Systems.

9.11[1] Counsel Should Review Data Retention Policy and Network Diagrams.

9.11[2] Counsel Should Understand Client's Document Management Systems.

9.11[3] Structured Data Systems Such As Accounting and Process Databases Present Special Issues.

9.11[4] Counsel Should Understand Client's E-Mail System.

9.11[5] Other Less Obvious Sources of ESI Can Also Contain Responsive Information.

9.12 Identifying Key Players With Information Relevant to Subject Matter of Dispute (Document Custodians).

9.13 Interviewing Key Document Custodians.

9.13[1] Counsel Should Interview Witnesses Regarding Their Role in Dispute.

9.13[2] Witnesses' Electronic Assets Should Be Identified and Catalogued.

9.13[3] Interviewing Witness About How Witness Works Enables Counsel to Determine Where Responsive ESI Is Likely to Reside.

9.14 Determining How ESI Is to Be Collected.

9.15 CHECKLIST: Negotiating With Opposing Counsel Regarding Production of ESI and Protection of Confidential Information.

9.16 Options and Strategy.

9.17 Negotiations With Opposing Counsel Often Begin Early in Process.

9.18 Stipulated Protective Orders Can Be Used to Protect Confidential and Proprietary Information.

9.19 CHECKLIST: Performing and Documenting a Diligent Search for Responsive ESI.

9.20 Options and Strategy.

9.21 Developing a Collection Plan and Documenting It With an Audit Trail.

9.21[1] Counsel Should Plan Ahead to Create a Collection Procedure That Will Withstand an Opponent's Challenge.

9.21[2] Counsel Should Develop Audit Trail of Collection Efforts.

9.22 Identifying Particular Custodians Likely to Have ESI Responsive to Document Demand.

9.23 Identifying Systems and Media Assets Likely to Contain ESI Responsive to Document Demand.

9.24 Deciding Who Should Gather the ESI and How They Should Do It.

9.24[1] Decision Involves Balancing Need to Preserve Evidence and Demands of Case.

9.24[1][a] Selection of Method Should Be Made on Case-by-Case Basis.

9.24[1][b] Custodian Self-Selection.

9.24[1][c] Guided or Centralized Search.

9.24[1][d] Forensic Recovery by Imaging Hard Drive or Other Means.

9.24[2] If ESI Issues Are Unlikely to Be Contested, Counsel May Be Able to Allow Client to Gather ESI.

9.24[3] Outside Expertise Should Be Considered When Metadata May Play a Critical Role in Case or Case Involves Allegations of Dishonesty.

9.24[4] Self-Selection of a Portion of ESI by Custodians May Be a Component of Collection Plan in Large Organizations With Complex Systems.

9.24[5] Counsel Should Preserve Ability to Retrieve Additional ESI.

9.25 Counsel Should Understand Metadata, Active Data, and Inactive Data.

9.26 Utilizing Appropriate Collection Methods to Preserve Metadata and Inactive Files If Necessary and to Identify and Gather Potentially Responsive ESI.

9.26[1] Manual Copy Has Potential to Alter File Level Metadata.

9.26[2] Active Data Copy Alters Directory Level Metadata but Not File Level Metadata.

9.26[3] Forensic Image Process Preserves Directory and File Level Metadata.

9.26[4] Forensic Data Capture Is Likely Necessary When Activity of User Is As Important As Content of Data.

9.26[5] Forensic Data Capture Is Likely to Be Necessary When Concerns Regarding Destruction of Data May Be Raised.

9.27 If Risk of Intentional Destruction Exists, Court May Order Collection and Preservation of ESI by Neutral Expert.

9.28 Narrowing Volume of Data to Review by Carefully Targeting and Limiting Media Assets to Be Harvested.

9.28[1] ESI Is Too Voluminous to Collect Indiscriminately.

9.28[2] Limiting Number of Witnesses Whose ESI Will Be Collected Limits Volume of ESI to Review.

9.28[3] Volume of ESI Can Be Further Reduced by Examining Whether Certain Types of Data Can Be Excluded.

9.28[4] Collecting a Defined Subset of Any Given Particular Data Type May Be Warranted.

9.28[5] Data Collected Can Be Further Reduced by Date-Restricting the Information Collected.

9.28[6] Keyword and/or Conceptual Searching May Be Used to Limit ESI Collections.

9.29 CHECKLIST: Analyzing Collected ESI to Narrow Scope of Data to Be Reviewed for Production.

9.30 Options and Strategy.

9.31 Developing an Analysis Plan.

9.32 Applying De-Duplication Techniques to Reduce Volume of Data.

9.33 Developing Systematic and Defensible Search Term Strategy to Reduce Review Set to a Manageable Volume of Documents.

9.33[1] Agreeing With Opposing Counsel on a Search Strategy Is Likely to Be Most Cost Effective.

9.33[2] Ad Hoc Searching Is Likely to Be Ruled Insufficient.

9.33[3] Carefully Crafted Search Strategy Allows Counsel to Demonstrate to Opposing Counsel and Court That Strategy Is Appropriate.

9.34 Counsel Should Consider Retaining Expert Assistance If Case Is Hotly Contested or Involves a Large Volume of Data in a Variety of Formats.

9.35 Developing Appropriate Queries for Gathering ESI From Databases.

9.36 CHECKLIST: Reviewing for Responsiveness and Privilege.

9.37 Options and Strategies.

9.38 Review Methodology and Software Depend on Budget and Needs of Case.

9.38[1] Manual Paper-Based Review May Be Appropriate in Limited Circumstances Involving Very Small Datasets.

9.38[2] Systems That Rely on Conversion of Documents to TIFF or PDF Format Prior to Review Have Commonly Been Used for Medium-Sized Cases.

9.38[2][a] Electronic Files Are Converted in Image Files.

9.38[2][b] Attorney Can Review Image Files Without Danger of Altering Them.

9.38[2][c] E-Mails Are Converted Into HTML or Plain Text Files.

9.38[2][d] User Categorizes Documents.

9.38[2][e] Cost of Conversion Is a Disadvantage.

9.38[2][f] Difficulty of Conversion Can Be a Disadvantage.

9.38[3] Some Vendors Offer Native File Review With TIFF Conversion on Demand.

9.38[4] Online Hosted Review Systems Allow Geographically Dispersed Teams to Effectively Review Large Amounts of Data While Maintaining Appropriate Audit Trail of Review Activities.

9.39 Counsel Should Evaluate Whether to Perform Case Assessment Concurrently With Review.

9.40 Components of an Effective Review Procedure.

9.41 Educating Review Team About Case and Privilege Issues.

9.41[1] Review Team Members Should Be Thoroughly Educated About Case.

9.41[2] Reviewing Attorneys Must Understand Relationships Between In-House Counsel, Outside Counsel, and Attorneys Not Affiliated With Client.

9.42 Attorney-Client Privilege and Attorney Work Product Privileges Are Easily Waived.

9.42[1] Voluntary Production of Privileged Material Waives the Privilege.

9.42[2] CCP § 2031.285 Provides a Method for Party Inadvertently Producing Privileged Information to Claw It Back.

9.43 Identifying and Segregating Privileged Information.

9.43[1] Stipulating With Opposing Counsel That ESI Belonging to In-House Counsel Need Not Be Searched or Produced Can Save Significant Resources.

9.43[2] Appropriate Search Terms Can Help Identify Privileged Documents.

9.44 Reviewing Documents Segregated As "Provisionally Privileged"

9.44[1] Holding Back Entire Documents That Are Privileged.

9.44[2] If Only Part of Document Is Privileged, Reviewing Platforms Should Provide Method to Specify Text to Be Redacted From Final Produced Image.

9.44[3] Listing Individual Privileges As Separate Issue Codes Can Speed Compilation and Editing of Privilege Log.

9.45 Reviewing Remaining Documents.

9.45[1] Remaining Documents Must Still Be Checked for Privilege.

9.45[2] Issue Codes Should Be Established Based on Elements of Case Identified During Review of Pleadings, Demurrers, and Model Jury Instructions.

9.46 Preparing Privilege Log.

9.47 CHECKLIST: Producing Documents to the Demanding Party.

9.48 Options and Strategy.

9.49 Demanding Party May Specify Form of Production.

9.50 Responding Party May State Form in Which It Intends to Produce ESI.

9.50[1] Responding Party Must Produce ESI in "Reasonably Usable" Form.

9.50[2] Initial Meet and Confer Should Have Addressed Production Format Issues.

9.51 Paper Production Is Only Appropriate for Smallest Datasets or When Agreed Upon by Opposing Counsel.

9.52 Production in TIFF or PDF Format Accompanied by Load Table of Agreed-Upon Metadata Is Common.

9.52[1] Production of ESI in TIFF or PDF Format Allows Information to Be Easily Utilized in Connection With Case Management Software.

9.52[2] Database Load File of Metadata Provides Relevant Information Concerning Document Image.

9.52[3] Documents Produced in TIFF or PDF Format May Easily Be Redacted and Control-Labeled.

9.52[4] TIFF and PDF Formats Have Some Disadvantages.

9.53 ESI Is Often Produced in Near-Native Format When Producing Large Compilations Derived From Searches of Large Databases.

9.54 Production of ESI in Native Format Is Least Expensive But Can Be Problematic.

9.54[1] Native ESI Can Be the Most Useful Format and Least Expensive for Production.

9.54[2] Native Format Production Presents Difficulties in Handling and Review.

9.55 Timing the Production of ESI.

9.55[1] Propounding Party May Not Specify Less Than 30 Days for Production of ESI.

9.55[2] Parties Should Agree to Production Schedule When Large Amounts of Data Are Likely to Require More Than 30 Days to Process and Produce.

9.55[3] Rolling Production May Meet Both Parties' Objectives.

9.55[4] Choosing a Location for Production.

9.56 Counsel Should Document Each Production With Cover Letter Detailing What Was Produced.

9.57 Sample Records Custodian Interview Checklist.

9.58 San Mateo County Superior Court Model Stipulation and Protective Order Regarding Confidential Information (Single Level of Confidentiality).

9.59 San Mateo County Superior Court Model Stipulation and Protective Order Regarding Confidential Information (Two Levels of Confidentiality).

9.60 Sample Letter to Opposing Counsel Documenting Information Produced.

Ernst Halperin n*

FOOTNOTES:

(n13)Footnote *. Law Office of Ernst Halperin, San Francisco. Previously a partner with the San Francisco firm of

Folger Levin & Kahn LLP, Mr. Halperin has litigated complex commercial, bankruptcy, and intellectual property cases since 1995. He has managed the discovery of ESI in cases alleging breach of merger agreements, trade secret misappropriation, fraudulent transfers, construction defects, and patent infringement. He currently practices as a dispute resolution neutral.



125 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

I. STRATEGY

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.01

AUTHOR: Ernst Halperin

9.01 Scope.

This chapter covers:

- Understanding the case [*see 9.03-9.06*].
- Preparing to gather ESI in response to a demand for production [*see 9.07-9.14*].
- Negotiating with opposing counsel regarding production of ESI and protection of confidential information [*see 9.15-9.18*].
- Performing and documenting a diligent search for responsive ESI [*see 9.19-9.28*].
- Analyzing collected ESI to narrow scope of data to be reviewed for production [*see 9.29-9.35*].
- Reviewing the reduced data set for responsiveness and privilege [*see 9.36-9.45*].
- Producing documents to opponent [*see 9.46-9.56*].



126 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
I. STRATEGY

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.02

AUTHOR: Ernst Halperin

9.02 Objective and Strategy.

The amount of information organizations can store electronically has grown dramatically in the past decade. Personal computers now routinely ship with internal disk drives in excess of 200 gigabytes. Retailers sell portable backup drives with a 1.5 terabyte capacity for less than \$150. How much information is that? 100 gigabytes is equal to an entire library floor of academic journals, or 100 pickup trucks full of books [Lyman, Peter and Hal R. Varian, "How Much Information," Table 1.1, 2003, retrieved from <http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/>]. The entire print collection in the Library of Congress contains 10 terabytes of information [Lyman, Peter and Hal R. Varian, "How Much Information," Table 1.1, 2003, retrieved from <http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/>]. Chevron's Chief Information Officer has stated that his company accumulates data at the rate of 2 terabytes a day--accumulating enough data during a work week to fill the entire Library of Congress [*Computerworld*, October 30, 2006, "Where Size Is Opportunity," p. 22].

The volume of ESI in an organization of any size is likely to far exceed the capacity of a law firm to manually gather and review it in response to a demand for production. Instead, it is necessary to develop a systematic approach for:

- Identifying the systems likely to contain the requisite information.
- Preserving the data.
- Narrowing the information reviewed down to a manageable size in a manner that is defensible if challenged by one's opponent.
- Reviewing the ESI for responsiveness and privilege.
- Timely producing the information.

The process of gathering and producing ESI can be thought of as a data funnel -- preserve broadly, collect less broadly, review even less broadly--produce more narrowly, but leave the ability to back up if challenged without having committed spoliation of evidence.

Counsel can be prepared to effectively implement this funneling technique by:

- Understanding the case in order to determine the important facts that each side will need to prove and thus what information one needs to gather.
- Understanding the client's organization, data systems, and where the ESI of key witnesses resides.
- Preserving ESI from routine destruction.
- Performing a diligent search for and collecting responsive ESI.
- Analyzing the collected ESI to narrow the scope of data to be manually reviewed for production.
- Reviewing the reduced dataset for responsiveness and to segregate privileged information.
- Producing the resultant non-privileged ESI to the demanding party in a reasonably useable form.

Consider--The Sedona Conference(R) and Electronic Discovery Reference Model:

The Sedona Conference(R) Working Group on Electronic Document Retention & Production (currently numbering more than 400 participants from academia, the bench, government, and the civil bar) has produced "Best Practices Recommendations & Principles for Addressing Electronic Document Production." (June 2007, The Sedona Conference(R)). The 14 principles enumerated in the report are often referred to as "The Sedona Principles." The report is the result of the Sedona Conference(R) Working Group's efforts since 2002 to address the issue of whether rules and concepts developed largely for paper discovery would be adequate to address issues of electronic discovery. The 2007 report is useful reading for any counsel preparing to deal with discovery of ESI. The Sedona Principles deal with many of the same issues addressed in California's Electronic Discovery Act as well as the 2006 e-discovery amendments to the federal rules. The resources and authorities attendant to the Comments to the Sedona Principles provide insight into how many courts across the country have dealt with these issues.

Similarly, the public domain Electronic Reference Discovery Model ("ERDM") (<http://www.edrm.net/>) is another good resource for counsel addressing issues of electronic discovery. The ERDM provides a technical process-flow based explanation of the electronic discovery process with recommendations for best practices. It is published on the web in a wiki format.



127 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

II. UNDERSTANDING THE CASE

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.03

AUTHOR: Ernst Halperin

9.03 CHECKLIST: Understanding the Case.

- ☐ Review complaint for plaintiff's factual allegations, theory of the case, and causes of action.

Discussion:

See 9.06[1]

- ☐ Review defendant's answer for affirmative defenses.

Discussion:

See 9.06[2]

- ☐ Review papers in support of and opposition to demurrers for additional information about the parties' themes.

Discussion:

See 9.06[3]

- ☐ Review CACI and BAJI model jury instructions for elements of causes of action and affirmative defenses.

Discussion:

See 9.06[4]

- ☐ Research case law for elements of causes of action not found in model jury instructions.

Discussion:

See 9.06[4]

- ☐ Review theory of the case.

Discussion:

See 9.06[5]

- ☐ Brainstorm regarding potential causes of action that could potentially be pleaded in order to understand the elements of those causes of action.

Discussion:

See 9.06[6]



128 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

II. UNDERSTANDING THE CASE

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.04

AUTHOR: Ernst Halperin

9.04 Options and Strategy.

Understanding the case in order to determine the important facts that each side will need to prove and thus what information one will need to gather is a necessary first step in developing and implementing an effective strategy for collecting and producing ESI.

If counsel has not already done so at the outset of the case, counsel should review the complaint, answer, any motions filed in the case, and the Judicial Council of California Civil Jury Instructions as soon as practicable after receiving a demand for production. All attorneys who are added to the team assembled for document review and production should also familiarize themselves with the case in the same manner.



129 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
II. UNDERSTANDING THE CASE

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.05

AUTHOR: Ernst Halperin

9.05 Civil Discovery Act Defines Parameters of Allowable Discovery.

California's Civil Discovery Act allows discovery of any information relevant to the *subject matter* of the pending action. Thus, the Act allows broad discovery. Under the Act, a party is entitled to discovery regarding any matter as long as it is:

- Not privileged;
- Relevant to the subject matter involved in the pending action or to the determination of any motion made in that action; and
- The matter either is itself admissible in evidence or appears reasonably calculated to lead to the discovery of admissible evidence.

Discovery may relate to the claim or defense of the party seeking discovery or of any other party to the action [CCP § 2017.010]. The California standard is broad, and California courts allow significant leeway, including a limited amount of "fishing expeditions" [*Calcor Space Facility v. Superior Court* (1997) 53 CA4th 216, 224, 61 CR2d 567 ("[t]hese rules are applied liberally in favor of discovery, and contrary to popular belief, fishing expeditions are permissible in some cases" [internal citations and parenthesis omitted])].

Compare--Civil Discovery Act Allows Broader Discovery Than Federal Rules:

The 2000 amendment to *Fed R Civ P 26(b)(1)* limited discovery under Federal practice to matter "relevant to any party's claim or defense" [*Fed R Civ P 26(b)(1)* (emphasis added)]. The 2000 amendment eliminated the language in Rule 26 that previously allowed discovery of information relevant to "the subject matter involved" in the action. "The rule change signals to the [federal] court that it has the authority to confine discovery to the claims and defenses asserted in the pleadings, and signals to the parties that they have no entitlement to discovery to develop new claims or defenses that are not already identified in the pleadings" [*Fed R Civ P 26(b)*, Committee Note 2000]. Nevertheless, the types of information that are discoverable even under the Federal Rules still are quite broad.

Example--Broad Discovery Under Federal Rule:

A federal magistrate judge granted a motion by the defendants to compel the plaintiff to identify whether

a certain internet protocol address was associated with his office email account. The court reasoned that the information was relevant to the question of whether the plaintiff, a lawyer by trade, was a "consumer" within the meaning of the Ohio Consumer Sales Practices Act under which he was suing the defendant for sending allegedly misleading email solicitations [*Ferron v. Subscriberbase Holdings, Inc.* (SD Ohio Mar. 22, 2010) 2010 U.S. Dist. LEXIS 34414] .



130 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

II. UNDERSTANDING THE CASE

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.06

AUTHOR: Ernst Halperin

9.06 Counsel Should Review Pleadings and Motion Papers That Frame the Issues.

9.06[1] Complaint Tells Plaintiffs' Story. The pleadings frame the issues being litigated. Motion papers in connection with demurrers often forecast the parties' case themes. Reviewing pleadings and motion papers before beginning the process of collecting ESI enables counsel to develop an understanding of the case necessary for developing an effective plan for gathering the ESI necessary to comply with discovery demands.

A complaint must contain "[a] statement of the facts constituting the cause of action, in ordinary and concise language" [CCP § 425.10(a)(1)]. The complaint is the plaintiff's first chance to educate the judge, and strategic counsel will often take full advantage of the opportunity to draft a pleading that tells a compelling story. Thus, a well-drafted complaint will often reveal the plaintiff's theory of the case and is a roadmap to the facts the plaintiff must prove at trial to prevail.

9.06[2] Answer Contains Defendants' Affirmative Defenses. The answer to an unverified complaint is often a general denial, which does not provide any useful information about the defendants' theory of the case. However, the party's "defenses shall be separately stated, and the several defenses shall refer to the causes of action which they are intended to answer, in a manner by which they may be intelligibly distinguished" [CCP 431.30(g)]. Evaluating the affirmative defenses allows counsel to determine the facts that the defendant will have to prove at trial in order to establish a defense.

9.06[3] Papers in Support of and Opposition to Demurrers Often Describe Parties' Themes. If the defendant has demurred to the complaint prior to filing an answer, the demurrer itself and the memorandum of points and authorities in support of the demurrer will often flesh out a portion of the defendant's theory of the case. Similarly, the plaintiff's papers in opposition to the demurrer often reveal its theory of the case.

9.06[4] CACI and BAJI Model Jury Instructions List Elements of Each Cause of Action and Affirmative Defense. Counsel most often use the new version of the Judicial Council of California Civil Jury Instructions (the "CACI" instructions) at trial. Some counsel and courts use the older Book of Approved Jury Instructions by the Civil Committee on California Jury Instructions (the "BAJI" instructions). The model jury instructions identify the necessary elements that a plaintiff must prove in order to prevail on a cause of action. The exercise of drafting a preliminary set of jury instructions based upon the model instructions will provide counsel with a roadmap to the facts likely to be at issue

in the case. This roadmap can be a useful checklist for counsel when thinking about which witnesses are likely to have information critical to the case, and what ESI might exist and be used in evidence at trial.

The CACI and BAJI instructions do not cover all potential causes of action under California law. If there is no model jury instruction for a cause of action pled in the complaint, case law research can be performed to determine the elements of the cause of action.



Warning:

The CACI and BAJI instructions are not always the most current correct statement of the law. A reported appellate case may change law upon which a model instruction was based, rendering the instruction incorrect. Counsel should Shepardize the cases cited in a model instruction to ensure that they remain good law.

9.06[5] Theory of Each Party's Case Provides Useful Information. The theory of the case is a short, easily understood theme for the trial that persuasively states the client's case. Every bit of evidence that is presented by a party at trial should be focused on proving the theory of the case. By thinking about both sides' theory of the case, counsel can be prepared to understand what facts (and thus what evidence) are likely to be most critical to each side's story.

9.06[6] Counsel Should Brainstorm Regarding Potential Causes of Action That Were Not Pleaded but Might Be Included in an Amended Complaint and Affirmative Defenses. Counsel should attempt to anticipate what causes of action are likely to be pleaded in any amended complaint, and to understand the elements of the causes of action. The same holds true for possible affirmative defenses to those causes of action. This exercise enables counsel to identify, and plan to preserve, evidence that has not been identified through analysis of the existing pleadings, but is likely to become important to the case in the future.



131 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

III. PREPARING TO GATHER ESI IN RESPONSE TO A DEMAND FOR PRODUCTION

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.07

AUTHOR: Ernst Halperin

9.07 CHECKLIST: Preparing to Gather ESI in Response to a Demand for Production.

- ☐ Consider whether to hire an ESI consultant.

Discussion:

See 9.09

- ☐ Meet with ESI gathering and production project team.

Discussion:

See 9.10

- ☐ Understand client's data systems.

Discussion:

See 9.11

- ☐ Identify key witnesses (document custodians)

Discussion:

See 9.12

- ☐ Interview key document custodians to:

- ☐ Determine their role in the dispute.
- ☐ Determine where their responsive ESI is likely to reside.

- ☐ Identify and catalog their electronic assets containing ESI.

Discussion:

See 9.13

Form:

See 9.68

- ☐ Determine how data is to be collected.

Discussion:

See 9.14



132 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

III. PREPARING TO GATHER ESI IN RESPONSE TO A DEMAND FOR PRODUCTION

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.08

AUTHOR: Ernst Halperin

9.08 Options and Strategy.

In order to comply with discovery obligations effectively and in a cost-efficient manner, counsel will need to develop a thorough understanding of how the client's electronic information systems are organized, who uses them, how they are used, and how ESI is maintained on the systems throughout its life cycle.

In an organization with in-house counsel, that counsel in most cases will be able to provide information about the client's data retention and litigation hold policies, and provide some information about the general structure of the client's electronic information systems and how ESI is used and stored. In-house counsel will also be able to provide outside counsel with access to the client's information technology personnel who can provide more detailed information about these issues.

Cal Rules Ct, Rule 3.724 requires counsel to meet and confer about issues related to the production of ESI no later than 30 days before the initial case management conference. If this has not already occurred by the time a demand for production of documents has been received, counsel should review the requirements of Rule 3.724 to become familiar with the basic issues surrounding the preservation and production of ESI that are likely to cause disputes. These include the preservation of discoverable ESI, the form or forms in which information will be produced, and the time within which the information will be produced. The client's in-house IT personnel, in-house counsel, and any ESI consultant engaged to assist in the discovery process are valuable resources in helping counsel understand the client's organization and electronic systems.



133 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

III. PREPARING TO GATHER ESI IN RESPONSE TO A DEMAND FOR PRODUCTION

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.09

AUTHOR: Ernst Halperin

9.09 Counsel Should Consider Whether Engaging an ESI Consultant Would Be Appropriate.

If, at the time a demand for production has been received, counsel has not already discussed with the client whether to engage an ESI consultant, this conversation should occur as soon as possible. If counsel and the client have substantial experience in responding to demands for ESI, retention of an ESI consultant may not be necessary. However, in many cases an ESI consultant who specializes in electronic discovery can be invaluable in providing assistance in designing and implementing an effective process for identifying, collecting, filtering, reviewing and producing ESI.

► **Cross Reference:**

Discussion of retaining an ESI consultant, see *Ch. 4, Planning E-Discovery, 4.11-4.14; Ch. 5, Initial Procedures in E-Discovery: Notice, Document Preservation, Meeting and Conferring, and Case Management Conference, 5.06[1]*.



134 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

III. PREPARING TO GATHER ESI IN RESPONSE TO A DEMAND FOR PRODUCTION

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.10

AUTHOR: Ernst Halperin

9.10 Counsel Should Meet With Client's In-House Counsel, IT Personnel, and ESI Consultant to Develop Data Collection Plan and Update Data Preservation Plan.

As soon as possible after receiving a demand for production, counsel should meet with the project team to develop a data collection plan. This meeting will cover many of the same issues as the meeting previously held to discuss data preservation, but this time with the benefit of a concrete set of requests that will enable the project team to identify particular document custodian's ESI for collection. As with the meeting to develop a data preservation plan, this meeting should preferably occur in person, but can also be done via conference call.

Topics counsel may want to cover during the meeting are:

- Identification of key witnesses (custodians) and the data systems that hold their ESI.
- Identification of other structured data systems likely to hold data responsive to the demand and implementation of a plan for production of that information.
- Discussion of whether the methodology for implementing the litigation hold needs to be modified or expanded in light of the particular demands for production.
- Planning for the collection of custodians' ESI.
- Timing and deadlines for each step of the process.

There are additional topics that one will want to cover with in-house counsel and the ESI consultant if they were not already covered earlier, but do not always require in-house IT personnel's involvement:

- Budget for gathering and processing ESI.
- Methodology for filtering ESI once it has been gathered in order to reduce it to a manageable size for review.

- Systems for reviewing and, when necessary, redacting the filtered ESI prior to production, and for creating privilege logs.

Finally, the project team should review the scope of the document preservation plan already in place, as well as all document preservation memoranda and reminders sent to individual custodians. Does the demand for production require gathering and preserving data from witnesses that were not previously anticipated? Is the subject matter of the demands broader than the subject matter of data that custodians have been admonished to preserve? Are previously unanticipated data systems now involved given the scope of the demand for production? Counsel should carefully analyze these issues, and adjust the data preservation plan accordingly.

**Strategic Point:**

If the scope of the discovery demands is different from previously anticipated, counsel should prepare a new document preservation reminder for the client to distribute to all document custodians incorporating the subject matter of the new set of demands for production.

**Cross Reference:**

Discussion of developing a plan for preservation of ESI, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferring, and Case Management Conference, 5.03-5.08*.



135 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

III. PREPARING TO GATHER ESI IN RESPONSE TO A DEMAND FOR PRODUCTION

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.11

AUTHOR: Ernst Halperin

9.11 Understanding Client's Data Systems.

9.11[1] Counsel Should Review Data Retention Policy and Network Diagrams. If counsel has not already done so in connection with planning for data preservation, counsel should review the client's data retention policies and network diagrams to gain an understanding of the client's data environment.

Counsel should review the data retention policy and network diagram as soon as possible after receiving a demand for production, and become familiar with these documents in advance of the project team meeting. Any members added to the document collection team should review these documents as soon as they join the team.

► Cross References:

Discussion of data retention policy, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference, 5.06[2]*.

Discussion of network diagrams, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference, 5.06[3]*.

9.11[2] Counsel Should Understand Client's Document Management Systems. Many organizations have a document management system that controls the creation and utilization of common electronic documents used in the organization. These systems often have the capability of creating an audit report of access, edits, versions, and copies of documents.

Although the goal of a document management system is to allow indexing and control of an organization's documents, one cannot assume it is truly comprehensive. Employees do not always use the document management systems correctly or consistently. Counsel should learn how the client's system may be bypassed, and how and where users store their documents if they circumvent the system.

9.11[3] Structured Data Systems Such As Accounting and Process Databases Present Special Issues. The information in structured data systems takes its meaning from the structure in which it is organized. The data itself, outside of its context, is often useless.

Example:

An example of a structured data system is an enterprise accounting software database.

Production of the raw data from structured data systems is not likely to qualify as production in a form that is "reasonably useable" under *CCP § 1985.8(c)(1)*. Instead, the responding party must, at the reasonable expense of the demanding party, translate any data compilations included in a demand into reasonably useable form [*CCP § 2031.280(e)*].

In-house counsel and the client's IT personnel can help counsel determine what information in a demand for production can be produced by running queries to the client's structured database systems.

If the client runs legacy mainframe computer systems, transaction data may be archived on tape. Counsel should become familiar with how far back the records are archived, and should inquire how easily archived data tapes can be re-loaded into the system to run inquiries. Understanding this issue thoroughly will ensure that counsel is armed with accurate information concerning the burdens of producing demanded information from structured data systems.

9.11[4] Counsel Should Understand Client's E-Mail System. The client's e-mail system will often be a central focus of electronic discovery, simply because an ever-increasing amount of business communication takes place via e-mail instead of by voice or letter. Counsel must develop enough knowledge about the system to be able to effectively gather e-mails for analysis. An ESI consultant can be especially helpful in understanding the client's systems.

Counsel also should learn how the users interact with the e-mail system. The client's IT personnel can often explain common user practices that counsel will want to explore when interviewing key individual witnesses (document custodians).

Example:

The Outlook e-mail system allows individual users to easily create an archive file (often referred to by its file extension as a PST file) on the computer's local hard drive or on other media such as a CDROM. Users in companies with e-mail size storage limits often create archive files of old e-mail before deleting e-mails from their active directories. If such archive files exist, they will need to be reviewed for production as they likely contain e-mails that have been "deleted" from the user's active mailbox.

9.11[5] Other Less Obvious Sources of ESI Can Also Contain Responsive Information. Central servers and individual desktop computers are not the only data assets that should be considered when identifying systems likely to contain responsive information. Employees of an organization who work from home may have responsive information on their home computers, laptop computers, flash drives, smart phones and personal digital assistants, and even their voice mail.

**Strategic Point.**

Counsel should carefully review the scope of opposing party's demand for production to determine whether these less obvious sources of data need to be searched. In most cases they will, because the broad definition of "electronically stored information" in *CCP § 2016.020* will encompass these forms. Moreover, although the scope of production will be framed by the scope of the demand, most demands today incorporate broad language asking for all information in the custody or control of the responding party, its agents, and its employees. Many demands for production also use lists of ESI definitions that include less obvious sources of ESI such as personal digital assistants, flash memory, and the like.

**Cross Reference:**

Sources of ESI, see Ch. 1, Understanding Electronic Evidence, Ch. 4, Planning E-Discovery, 4.03, 4.10.

Demand for production of ESI listing all ESI sources to be produced, see *Ch. 6, Demanding Production of Electronically Stored Information in California Court*, 6.03-6.08.



136 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
III. PREPARING TO GATHER ESI IN RESPONSE TO A DEMAND FOR PRODUCTION

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.12

AUTHOR: Ernst Halperin

9.12 Identifying Key Players With Information Relevant to Subject Matter of Dispute (Document Custodians).

A major factor in the cost of electronic discovery is the number of document custodians whose information is gathered and searched. A party receiving a demand for production has a duty to conduct a "diligent search and reasonable inquiry" [CCP § 2031.230]. The first step is identifying the key witnesses:

- People whose names appear in the narrative portion of a complaint, or who are named in interrogatory responses, are an obvious first set of key witnesses.
- In-house counsel (or the client's main representative for the matter if there is no in-house counsel) should be consulted for the names of other people likely to have information responsive to the document demand.
- Witnesses should be asked who else has information as part of their interview.

Strategic Point:



Counsel should consider whether the number and identity of custodians who need to respond to discovery can be limited by agreement with opposing counsel (either in initial case management meet and confer sessions or in response to discovery demands), objections on the basis of burden, and/or a court order.

Example:

For example, in a breach of contract case, the parties might agree to limit discovery to a core group of custodians on each side who had responsibility for the contract.

Strategic Point:



Broad discovery demands that ask for every version of a widely distributed piece of ESI often are not necessary, and may be reasonably limited in the response. For example, a demand for a corporation's

quarterly financial reports, if interpreted literally, may require gathering similar information from hundreds of custodians who might receive the financial information by e-mail. Rather than gathering from all these custodians, counsel should object to the broad demand, and instead produce a single set of "documents sufficient to identify" the financial information sought.

**Warning:**

Counsel should consult in-house counsel and document witnesses about potential sources of documents that have no identified custodian, such as former employees' files.

Example:

Defendant was late in producing 53 documents that were stored in a former employee's folder on a shared drive. Defendant's strategy to search the directories of only certain identified custodians had not initially identified the documents. The federal district court held that sanctions against defendant were appropriate because, when it became apparent to defendant that the search procedure had a major flaw--namely, a directory full of potentially relevant documents with no custodian--it was not reasonable for defendant to ignore the problem [*Wixon v. Wyndham Resort Dev. Corp.* (ND Ca 2009) 2009 U.S. Dist. LEXIS 86337 *13] .



137 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

III. PREPARING TO GATHER ESI IN RESPONSE TO A DEMAND FOR PRODUCTION

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.13

AUTHOR: Ernst Halperin

9.13 Interviewing Key Document Custodians.

9.13[1] Counsel Should Interview Witnesses Regarding Their Role in Dispute. As soon as possible after the project team has met to develop a plan for collecting ESI, interviews of key witnesses should begin.

Interviewing key witnesses is essential to understanding the facts of the case, what the factual disputes are between the parties, and who else has knowledge about the dispute. Moreover, understanding the role each witness plays in the subject matter of the dispute enables counsel to identify what categories of documents in their custody are likely to have information relating to the subject matter of the dispute and responsive to a demand for production.

9.13[2] Witnesses' Electronic Assets Should Be Identified and Catalogued. Cataloging the witnesses' electronic assets provides counsel with documentation of the reasonableness of the search. It also provides counsel with a checklist for a discussion with the witness about how the witness works. Common electronic assets are:

- Network folders.
- E-mail client on the witness's computer.
- Personal digital assistants.
- Smart phones (Blackberry, Treo, iPhone).
- Laptop computers.
- Home computers.
- Portable storage media such as thumb-drives, CD-ROM, portable backup drives.

9.13[3] Interviewing Witness About How Witness Works Enables Counsel to Determine Where Responsive ESI Is Likely to Reside. The interviewer should have the witness explain how the witness works, how he or she utilizes

the electronic assets catalogued, and how he or she interacts with the company's electronic data systems:

- **E-mail:** How does the witness use the company's e-mail system? Does the witness back up e-mails onto the local hard drive to circumvent any limitations on the size of active mailboxes? If so, counsel will want to ensure that those archive files are included in any search for responsive e-mails. Does the witness have an e-mail folder where he or she stores relevant information related to the matter? (The existence of such a folder may allow the basis of an argument for limiting production to that folder to reduce the burden of reviewing other sources such as the entire e-mail collection for that witness.)

- **Office documents:** Does the witness always use the organization's document management system? If not, where does the witness store documents--on a shared folder on the network? In a folder on a local hard drive?

- **Work out of the office:** Does the witness send or receive documents using a personal e-mail account if the witness is working from home? Does the witness use a laptop when working outside the office? Does the witness use a smart phone or personal digital assistant for work? Does the witness carry work on flash disks or thumb drives when taking it out of the office?

- **Other systems storing ESI:** Has the witness used instant messaging, texting, blogs, voice mail, Twitter, or any other service that might have stored information relevant to the matter?

Asking these questions allows counsel to identify potential sources of ESI that might otherwise be missed.



Cross Reference:

Form, see 9.60.



138 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
 III. PREPARING TO GATHER ESI IN RESPONSE TO A DEMAND FOR PRODUCTION

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.14

AUTHOR: Ernst Halperin

9.14 Determining How ESI Is to Be Collected.

As with paper-based collections, ESI is usually given to counsel for review and production by making a copy of the data. ESI collection differs from collection of paper-based documents in that the process of copying the data itself can alter it. Additionally, the ESI created by an organization may be orders of magnitude more voluminous than the volume of paper.

Example--Considerations in Collecting E-Mail:

The considerations that arise in collecting ESI can be illustrated by considering e-mail systems. With e-mail systems, common methods of copying include dragging and dropping of copies to a network folder, making an Outlook folder, making an entire PST of an Outlook folder, and forwarding e-mails. Occasionally forensic copying of data from a hard drive is performed. Each of these methods has benefits and drawbacks, and each has different effects on the ESI. Copying the data can alter it, and counsel should understand what alteration would be done by the copying method, and whether the alteration will be important to the case.

Another important issue is how to limit the gathering of e-mail so as not to overwhelm the review team, while ensuring that the client complies with the duty to perform a reasonable search. Will search terms be applied to identify documents and limit the collection? Will just certain folders be searched? How can these limits be defended? Is there an agreement with opposing counsel or a court order as to search terms that will prevent second guessing later and costly do-overs? If not, should counsel try to get an agreement or order before collecting, or, alternatively, should counsel overcollect so that uncollected data is not destroyed after too narrow a collection?

Counsel also needs to consider who will do the collection. Can the collectors testify and defend what they did, and how will counsel be able to prove that the collection was reasonable and complete?

All of these issues will need to be considered for not only e-mails, but for all types of ESI in the client's organization.



Cross Reference:

Discussion of who should gather ESI and how they should do it, see 9.35. Discussion of understanding

metadata, active data, and inactive data, see 9.50-54.

Discussion of utilizing appropriate collection methods to preserve metadata and inactive files, see 9.29-9.35. Discussion of narrowing the volume of data by targeting and limiting media assets to be harvested, see 9.29-9.35



139 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

IV. NEGOTIATING WITH OPPOSING COUNSEL REGARDING PRODUCTION OF ESI AND PROTECTION OF
CONFIDENTIAL INFORMATION

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.15

AUTHOR: Ernst Halperin

**9.15 CHECKLIST: Negotiating With Opposing Counsel Regarding Production of ESI and Protection of
Confidential Information.**

- ☐ Negotiate issues related to scope of product, form of production, and timing of production with
opposing counsel.

Discussion:

See 9.17

- ☐ Protect confidential and proprietary information with stipulated protective orders.

Discussion:

See 9.18



140 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

IV. NEGOTIATING WITH OPPOSING COUNSEL REGARDING PRODUCTION OF ESI AND PROTECTION OF
CONFIDENTIAL INFORMATION

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.16

AUTHOR: Ernst Halperin

9.16 Options and Strategy.

Counsel should negotiate issues of scope of the document collection with opposing counsel as soon as counsel has interviewed the client and understands the issues. Counsel also will want to negotiate issues related to the timing of the production, the form or forms in which ESI will be produced, cost allocation issues, and the method for protecting confidential information.

► **Cross Reference:**

Preparation and conduct of meet and confer process, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferring, and Case Management Conference*, 5.14-5.21.



141 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

IV. NEGOTIATING WITH OPPOSING COUNSEL REGARDING PRODUCTION OF ESI AND PROTECTION OF CONFIDENTIAL INFORMATION

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.17

AUTHOR: Ernst Halperin

9.17 Negotiations With Opposing Counsel Often Begin Early in Process.

Many general issues related to production of ESI may have already been negotiated as part of the mandatory e-discovery conference required by *Cal Rules Ct., Rule 3.724(8)*. If the meeting has not yet occurred, counsel should schedule a meeting to discuss the issues required under Rule 3.724(8). These topics include:

- Any issues relating to the preservation of discoverable electronically stored information.
- The form or forms in which information will be produced.
- The time within which the information will be produced (in many productions, it is simply not possible to collect, reduce, review, and produce ESI within the 30-day minimum time period provided by *CCP § 2031.030(a)(2)*).
- The scope of discovery of the information.
- The method for asserting or preserving claims of privilege or attorney work product, including whether such claims may be asserted after production.
- The method for asserting or preserving the confidentiality, privacy, trade secrets, or proprietary status of information relating to a party or person not a party to the civil proceedings.
- How the cost of production of electronically stored information is to be allocated among the parties.
- Any other issues related to the discovery of electronically stored information, including developing a proposed plan relating to the discovery of the information.

Strategic Point:



Negotiating the scope of the document collection with opposing counsel is likely to be the most cost

effective method for limiting the cost of e-discovery. If the number of custodians from whom information must be collected and processed can be limited by agreement or court order, the cost and time for document collection and analysis will be reduced. Similarly, a search term agreement that ESI need only be reviewed if it is found with certain search terms can limit the scope and cost of review. Careful thought should be given to proposed limits, and it may be well worth counsel's time to spend effort negotiating these issues with opposing counsel.

 Cross Reference:

Discussion of determining how ESI is to be collected, see 9.14.

Discussion of narrowing volume of data to review by targeting and limiting media assets and witnesses, see 9.29-9.35.

Discussion of issues likely to arise in connection with e-discovery conference, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference*, 5.18.



142 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

IV. NEGOTIATING WITH OPPOSING COUNSEL REGARDING PRODUCTION OF ESI AND PROTECTION OF CONFIDENTIAL INFORMATION

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.18

AUTHOR: Ernst Halperin

9.18 Stipulated Protective Orders Can Be Used to Protect Confidential and Proprietary Information.

If counsel has not already negotiated a stipulated protective order during a Rule 3.724(8) e-discovery conference, counsel for the producing party should propose a protective order. This should be done soon after receiving a demand for production implicating confidential information to allow entry of the order in advance of the due date for the document production.

Stipulated protective orders allow a party (or non-party to the proceeding who is producing information pursuant to a third-party subpoena) to protect information that is confidential or proprietary.



Warning:

Just because a protective order is in effect for discovery does not mean that the parties can file documents in court under seal by stipulation alone [*Cal Rules Ct, Rule 2.551(a)*]. Rather, documents filed in a court file may only be sealed if the court expressly finds facts that establish all of the following [*Cal Rules Ct, Rule 2.550(d)*]:

- There exists an overriding interest that overcomes the right of public access to the record.
- The overriding interest supports sealing the record.
- A substantial probability exists that the overriding interest will be prejudiced if the record is not sealed.
- The proposed sealing is narrowly tailored.
- No less restrictive means exist to achieve the overriding interest.

**Strategic Point:**

It would be too cumbersome and a waste of effort to seek court review of every designation of a document as "confidential," especially since most documents produced in litigation are never used as evidence in court. A properly crafted stipulated protective order can allow parties to designate documents as "confidential," while providing a mechanism for judicial review of the designation if the document is going to be filed with the court.

A well-crafted stipulated protective order should have a provision to allow third parties whose ESI has been subpoenaed, and not just the parties themselves, to designate documents as protected pursuant to the order. In routine cases where it is not necessary to shield information from the parties themselves, an order with one level of confidentiality can be used. If the case may involve information that is so sensitive it must be shielded from the opposing parties, a two-level order can allow parties to designate certain material as "highly confidential" or "attorneys' eyes only" so that it may be viewed only by attorneys and independent outside experts, and not by the opposing party's employees.

Some courts provide model stipulated protective orders that are designed to comply with the requirements of *Cal Rules Ct, Rules 2.550* and *2.551*. This publication reproduces the San Mateo County Superior Court Complex Civil Litigation Program model stipulations and protective orders for single and double levels of confidentiality. These orders may be used as models for attorney-drafted orders in other jurisdictions that do not have their own model forms.

**Cross References:**

Discussion of method for asserting or preserving confidentiality, privacy, trade secrets, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferring, and Case Management Conference*, 5.19

Form, San Mateo County Superior Court Model Stipulation and Protective Order Regarding Confidential Information (Single Level of Confidentiality), see 9.58.

Form, San Mateo County Superior Court Model Stipulation and Protective Order Regarding Confidential Information (Double Level of Confidentiality), see 9.59.



143 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

V. PERFORMING AND DOCUMENTING A DILIGENT SEARCH FOR RESPONSIVE ESI

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.19

AUTHOR: Ernst Halperin

9.19 CHECKLIST: Performing and Documenting a Diligent Search for Responsive ESI.

- ☐ Develop a collection plan and document it with an audit trail.

Discussion:

See 9.21

- ☐ Identify custodians, systems, and media assets likely to have responsive ESI.

Discussion:

See 9.22-9.23

- ☐ Decide who should gather ESI and how they should do it.

Discussion:

See 9.24

- ☐ Understand metadata, active data, and inactive data, and utilize appropriate collection methods.

Discussion:

See 9.25-9.26

- ☐ Narrow the volume of data to review by carefully targeting and limiting media assets to be harvested.

Discussion:

See 9.28



144 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

V. PERFORMING AND DOCUMENTING A DILIGENT SEARCH FOR RESPONSIVE ESI

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.20

AUTHOR: Ernst Halperin

9.20 Options and Strategy.

A party responding to discovery has a duty to conduct a diligent search and a reasonable inquiry [CCP § 2031.230]. However, the great advantage of ESI--the ability to store large amounts of data--is also its greatest disadvantage when it comes to document collection for discovery. Counsel must develop a collection plan that is designed to target the data most likely to be responsive to a demand for production and of most use in the lawsuit, but which also narrows as much as possible the scope of the document collection to make review feasible. The ESI must also be collected in a manner that does not alter or destroy evidence critical to the case. Careful planning, based upon a thorough understanding of the case, the role of key witnesses in the case, and the technological issues will enable counsel to accomplish these goals.



145 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
V. PERFORMING AND DOCUMENTING A DILIGENT SEARCH FOR RESPONSIVE ESI

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.21

AUTHOR: Ernst Halperin

9.21 Developing a Collection Plan and Documenting It With an Audit Trail.

9.21[1] Counsel Should Plan Ahead to Create a Collection Procedure That Will Withstand an Opponent's Challenge. Counsel should plan ahead to defend the collection plan and procedure chosen, and, if necessary, procure expert witnesses who can testify as to how the ESI was gathered and the reasonableness of the method used.



Strategic Point:

Each party has a duty to conduct "a diligent search and a reasonable inquiry" in response to a demand for production [see *CCP § 2031.230* (party asserting an inability to comply with a "demand for inspection, copying, testing, or sampling, shall affirm that a diligent search and a reasonable inquiry has been made in an effort to comply with that demand")]. If there are discovery disputes, opposing counsel will most often assert that the search has not been diligent. By planning ahead to develop a well-reasoned collection plan, counsel can prepare to successfully defeat such a challenge.

A well-reasoned collection plan should do the following:

- Identify the key custodians and their role in the case:
 - ☐ Describe what media assets associated with each custodian will be harvested.
 - ☐ Specify what portions of the ESI located on each media asset of each custodian will be harvested.
 - ☐ Describe who will do the collecting of the data.
- Identify data not associated with particular custodians (such as databases):

☐ Define the process for extracting the data from the source (e.g., lists any database queries to be used, define the output format, etc.)

☐ Describe who will do the data extraction.

- Define a protocol for how each type of ESI will be collected (e.g., "drag and drop," active data collection, forensic imaging, etc.).

- Set forth a realistic schedule for the collection effort.

- Define a procedure for tracking what has been collected, documenting when, from whom, by whom, and how.

9.21[2] Counsel Should Develop Audit Trail of Collection Efforts. A well-reasoned collection plan is only the first half of what is required to successfully withstand a challenge that a diligent search and reasonable inquiry has not been made. The *execution* of the plan must be documented as well. Counsel should develop a systematic method of documenting the information about ESI gleaned from interviews of document custodians.

When ESI is actually gathered, whoever is gathering it should document what they have done, in order to develop an audit trail and chain of custody. The person gathering the ESI also needs to be prepared, if necessary, to testify in court concerning the adequacy and reliability of the collection process.

The Electronic Data Reference Model recommends the following minimum information for properly maintaining a chain-of-custody log for original media such as hard drives, backup tapes, CDs, and DVDs [see EDRM (edrm.net), Collection--Guidelines > Auditability > Original Media]:

- A unique media ID. This becomes the core tracking number and all of the information extraction from the media.

- Date and time of receipt or collection of the evidence.

- The name of the person(s) collecting and/or taking possession of the evidence.

- A description of the type of evidence (e.g., 8mm tape, hard drive, etc.).

- A description of what the evidence represents (e.g., Exchange server--Chicago).

- Any label information (exact).

- Serial numbers.

- Description of the physical location at the time of possession.

- Areas for transferring possession of the media within the collecting organization or to a vendor.

- Description of collection methodology.

- Detailed description of data harvested on site.

- Check lists related to any on-site filtering of data during collection.

These media asset chain of custody logs should also show which witness is associated with each media asset. In the event that the custodian's work has been identified for ongoing collection, the collector must be able to identify what was collected on each visit and not collect the same, unchanged data, multiple times. In large collection projects involving many media assets belonging to many different custodians, the chain-of-custody information should be organized in a database to ensure that the records are easily retrievable and useable [see Electronic Data Reference Model (EDRM) (edrm.net), Collection--Guidelines > Auditability > Original Media].



146 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
V. PERFORMING AND DOCUMENTING A DILIGENT SEARCH FOR RESPONSIVE ESI

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.22

AUTHOR: Ernst Halperin

9.22 Identifying Particular Custodians Likely to Have ESI Responsive to Document Demand.

Counsel should have already identified a preliminary set of key witnesses as part of the process of preserving ESI. Key witnesses are likely to include:

- People whose names appear in the narrative portion of a complaint.
- People named in interrogatory responses.
- People identified by in-house counsel (or the client's main representative for the matter if there is no in-house counsel) as having information relevant to the subject matter involved in the pending action.
- People identified by key witnesses during their interviews as having relevant information.

The documents of already-identified key witnesses may also provide further leads in identifying other people with information relevant to the suit. For this reason, it is important, during document review, to maintain a system to keep track of witnesses. As new names appear in the documents being reviewed, an informed decision can be made about whether their electronic media assets should be collected for review as well.



Strategic Point:

A case analysis tool such as CaseMap can help in this regard by allowing counsel to easily link key documents to witnesses.



147 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

V. PERFORMING AND DOCUMENTING A DILIGENT SEARCH FOR RESPONSIVE ESI

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.23

AUTHOR: Ernst Halperin

9.23 Identifying Systems and Media Assets Likely to Contain ESI Responsive to Document Demand.

As with the identification of key custodians, counsel's review of the client's data systems and architecture for purposes of preservation of ESI should have identified the media assets likely to contain responsive ESI, whether they are structured data systems, witnesses' network data, and their off-network media assets such as personal digital assistants, smart phones, etc.

Although the key custodians' review of media assets for preservation purposes was very broad, during the collection phase the focus should be on identifying the ESI which is responsive to the particular document demand. Nevertheless, the techniques and inquiry are the same as before.

Cross References:

Discussion of understanding client's data systems, see Ch. 9.11.

Discussion of interviewing key document custodians, see 9.13.



148 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
V. PERFORMING AND DOCUMENTING A DILIGENT SEARCH FOR RESPONSIVE ESI

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.24

AUTHOR: Ernst Halperin

9.24 Deciding Who Should Gather the ESI and How They Should Do It.

9.24[1] Decision Involves Balancing Need to Preserve Evidence and Demands of Case.

9.24[1][a] Selection of Method Should Be Made on Case-by-Case Basis. ESI should always be gathered, searched, culled, reviewed, and produced in a manner that finds and identifies the necessary ESI, and does not alter or destroy potentially relevant evidence. There are a number of options for identifying and gathering ESI. Which option counsel chooses in any particular situation depends upon the issues in the case, the cooperativeness of opposing counsel, and the technological sophistication of the client.



Warning--Cost Increases With Level of Complexity:

The cost and burden increases as one moves toward more comprehensive methods and use of more expertise in the gathering. Costs also increase dramatically as more information is gathered that must be culled and, ultimately, reviewed by counsel. It naturally follows that the fewer media assets requiring searching, the less expensive the review. However, one gains defensibility of one's methods as one moves to more complete methods.

9.24[1][b] Custodian Self-Selection. The first option is custodian self-search, selection, and collection. This method is analogous to pre-ESI discovery, in which the client searched his or her own paper files and produced what was called for.



Cross Reference:

Discussion of allowing client to gather ESI, see 9.24[2].

9.24[1][c] Guided or Centralized Search. A second option is guided or centralized search and/or selection. Choices here include identifying ESI by custodian storage method, searching certain e-mail folders for key search terms, or searching the custodian's entire disk or e-mail. In the first alternative under the second option, a subset of the custodian's files is chosen from particular network directories or e-mail system folders. If the ESI in the relevant subfolder is so voluminous that reviewing all the e-mails in the subfolder for responsive documents would be

impractical, the subfolders can be searched using keywords.

If counsel is uncertain that the custodians follow the firm's stated protocol for organizing e-mails or information, keyword searching of the custodian's entire Outlook file or hard drive may be necessary.



Warning:

Keyword searching to narrow the scope of the collected ESI leaves data behind. If the collecting party is challenged on the adequacy of its search and later required to go back, the data left behind may have been lost or destroyed in the interim, leading to spoliation claims. Thus, unless the use of specific search terms and methods has been agreed upon, it is usually better to collect more broadly and narrow the reviewed set later with search terms.

The person performing the search must have the technical knowledge to understand the limitations of the search technique utilized, and must be able to perform the search competently.

Examples--Limitations of Search Techniques:

- Outlook's internal search function may miss files, and generally it should not be used to narrow a collection. Rather, the Outlook e-mail data should be collected more broadly, and then narrowed later using the more sophisticated searching tools available in litigation document review software.
- Files that do not have rendered text (a scanned PDF file that has not had optical character recognition routines performed on the image) will be missed in keyword searches. To the extent that such files include computer-readable images of text (e.g., typewritten text), this text may be deciphered and rendered searchable by running optical character recognition ("OCR") software on the images.
- Searches may not detect relevant documents that include typographical errors or incorrect optical character recognition ("OCR") results.

9.24[1][d] Forensic Recovery by Imaging Hard Drive or Other Means. The most comprehensive and expensive method for gathering ESI is forensic recovery through imaging of the custodian's hard drive or other means. This involves having a technician connect a drive to the computer with special forensic capture software that copies an "image" of the computer's hard drive.



Strategic Point:

Some types of imaging software can be set to exclude large numbers of irrelevant files such as the program files installed on the computer during setup. (This process is called "deNISTing"--NIST refers to the National Institute of Science and Technology (NIST), which manages a list of known software signatures.) Excluding irrelevant files from the NIST list reduces the number of files to be reviewed, and can reduce the cost of review when the client is paying by the gigabyte of collected data for processing.

Consider:

The use of forensic data capture techniques is most common in criminal cases, in which the defendant is less likely than in civil cases to stipulate to the authenticity of documents and the prosecution must be able to show an unbroken chain of custody and demonstrate that the evidence was not altered. Nevertheless, the techniques are becoming more frequently used in data collection for civil cases as the costs of hard drive storage continues to fall, and as e-discovery vendors promote their use [see Katz,

Forensic Collections in E-Discovery, 52 Orange County Lawyer 18 (March 2010)] .

9.24[2] If ESI Issues Are Unlikely to Be Contested, Counsel May Be Able to Allow Client to Gather ESI.

Self-selection of ESI by custodians may be acceptable for smaller organizations and simple systems if ESI issues are unlikely to be contested (that is, when thoroughness of collection is unlikely to be second-guessed, and metadata such as file access or modified dates are unlikely to be important evidence).

If the client gathers its own ESI, counsel still needs to guide the process and make sure that witnesses can testify as to what was done. Counsel should ensure that the document custodians understand what to do in finding and collecting ESI, and that counsel understands what has been done and can defend the process. The witnesses should be instructed in methods for gathering the ESI that disturb the metadata as little as possible. Counsel also should ensure that the witnesses will be prepared to testify about the collection process if necessary, should chain-of-custody issues arise. Allowing a client to gather ESI without guiding the process is not likely to be seen as fulfilling the client's responsibility to conduct a reasonable search for ESI.

Example:

In *Wachtel v. Health Net, Inc. (DNJ 2006) 239 FRD 81, 92*, the court held that "Health Net's process for responding to discovery demands was utterly inadequate" when Health Net relied on the document custodians themselves to turn over documents. Outside counsel did not verify that the searches were specific, and many of the custodians "managed to exclude inculpatory documents that were highly germane to Plaintiffs' requests" [*Wachtel v. Health Net, Inc. (DNJ 2006) 239 FRD 81, 92*] .



Strategic Points:

- Unless an agreement has been reached with opposing counsel, an attorney cannot know definitively whether ESI issues will be contested. The attorney should discuss these tradeoffs with the client and choose the methods that are defensible and cost-effective in light of issues in the case. Counsel may need to go to the court to get clearance for methods if the risk and cost justify it and the opposing counsel will not stipulate.
- The earlier these issues can be addressed, the better. Identifying and raising these issues early in the e-discovery conference and seeking case management or protective orders that limit discovery in reasonable ways will save all parties substantial sums of money.



Cross References:

Discussion of preparing for an e-discovery meet and confer conference, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference, 5.16*.

Discussion of negotiating limits on the scope of discovery at the e-discovery meet and confer conference, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management, 5.19[5]*.

Authentication and other evidentiary issues regarding ESI, see *Ch. 15, Admissibility of Electronic Evidence at Trial*.

9.24[3] Outside Expertise Should Be Considered When Metadata May Play a Critical Role in Case or Case Involves Allegations of Dishonesty. Serious consideration should be given to bringing in outside expertise for ESI

collection when metadata may become important in the case and counsel is not certain that the client is capable of collecting ESI without corrupting the metadata. If counsel and the client are not familiar with ESI and the governing law, this also weighs towards bringing in additional expertise from outside experts.

Self-selection by the client or custodian also is not recommended in disputes involving allegations of fraud or other dishonest action on the part of a custodian. Allowing custodians who have been accused of dishonesty to select and collect the documents to be reviewed invites opposing counsel to attempt to make spoliation of evidence claims.

9.24[4] Self-Selection of a Portion of ESI by Custodians May Be a Component of Collection Plan in Large Organizations With Complex Systems. Even when it is determined that outside expertise should be utilized, there may be a role for some self-selection of subsets of data by custodians. This may be as simple as instructing custodians to move documents or e-mails into a newly created folder for document collection. Counsel and any outside consultants should instruct the custodians in the proper method for accomplishing this without corrupting metadata that may be critical to issues in the case.

9.24[5] Counsel Should Preserve Ability to Retrieve Additional ESI. To the extent possible, when counsel has not received definitive clearance for a collection method, counsel should preserve the ability to go back later and retrieve additional ESI if ordered to do so. If a collection method is judged to be incomplete, and the additional uncollected ESI has been destroyed in the interim, the client may face spoliation of evidence claims with attendant sanctions. This leads to the rule of preserving broadly, even if one later decides to produce narrowly.

Cautious counsel should also preserve the ability to go back later and retrieve additional ESI even when counsel does not anticipate a fight about the completeness of document collection efforts. A party propounding a demand for production can propound supplemental demands for later acquired or discovered evidence twice before the initial setting of a trial date, and once after the initial setting of a trial date [*CCP* § 2031.050(b)]. Thus, it is important to be able to preserve the ability to retrieve additional ESI.



149 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

V. PERFORMING AND DOCUMENTING A DILIGENT SEARCH FOR RESPONSIVE ESI

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.25

AUTHOR: Ernst Halperin

9.25 Counsel Should Understand Metadata, Active Data, and Inactive Data.

Counsel should have a basic understanding of the fundamental concepts of metadata, active data, and inactive data in order to be able to make an informed, well-reasoned choice about the data collection method to utilize for any particular case. Counsel also needs to understand the metadata, active data, and inactive data for the different ESI types that key custodians have created, in order to make a reasoned decision about what metadata, active, and inactive data are likely to provide information relevant to issues in the litigation.

Cross References:

Definitions of active data and metadata, see Ch. 1, Appendix A, Glossary of Technical Terms Found in E-Discovery.

Discussion of metadata, see *Ch. 1, Understanding Electronic Data, 1.22[3]*.



150 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

V. PERFORMING AND DOCUMENTING A DILIGENT SEARCH FOR RESPONSIVE ESI

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.26

AUTHOR: Ernst Halperin

9.26 Utilizing Appropriate Collection Methods to Preserve Metadata and Inactive Files If Necessary and to Identify and Gather Potentially Responsive ESI.

9.26[1] Manual Copy Has Potential to Alter File Level Metadata. A person performing a manual copy of files uses operating system commands to make duplicates of the files, which can then be burned onto a CD or placed on a network folder. In the Windows environment, the user would select files, and use the "copy" and "paste" commands to accomplish the task. This technique alters the directory-level metadata, but ordinarily will not alter the file-level metadata. However, if the user opens a document in the process of reviewing it for responsiveness, the file-level metadata will be altered.

The main concern with the manual copy technique is that the quality of the copied data is dependent upon the operator performing the functions correctly. It is much easier to modify or corrupt the data being collected when the data is collected through a manual process than through an automated process. In addition, manual collection of ESI is not easily subject to authentication or verification. For these reasons, it is much easier for opposing counsel to attack the adequacy of a manual data collection, especially if any files have become corrupted or altered in the process.

Manual data copy does not allow deleted files to be retrieved. The operator relies upon what is visible to the computer's operating system, and deleted files are not visible to the operating system, even though they may still reside on the hard drive [see Electronic Data Reference Model (EDRM) (edrm.net), Collection Methods, http://edrm.net/wiki/index.php/Collection_-_Processes#Collection_Methods].

9.26[2] Active Data Copy Alters Directory Level Metadata but Not File Level Metadata. Active data copy techniques rely upon computer programs, rather than a user interacting manually with the computer's operating system, to make copies of data. Active data copy techniques alter the directory-level metadata, but leave file-level metadata intact. Active data copy techniques are a generally accepted method of collecting data when the data itself, and not the activity of the user, is the main concern in the litigation.

Active data collection techniques do not capture "inactive data" such as deleted files. If there are any allegations in a case about a document custodian's purposeful or inadvertent destruction of data, active copy techniques will not provide evidence to confirm or contradict the allegations [see Electronic Data Reference Model (EDRM) (edrm.net), Collection

Methods, http://edrm.net/wiki/index.php/Collection_-_Processes#Collection_Methods].

9.26[3] Forensic Image Process Preserves Directory and File Level Metadata. Forensic image collection from a hard-disk preserves both directory and file level metadata. Forensic image collection techniques also collect inactive data such as deleted files. They require specialized knowledge, and are generally the most expensive means of collecting data. Since they are used when the activity of the document custodian is at issue, best practices call for using a third-party consultant who is experienced in the methodology and can testify in court about the adequacy of the collection effort [see Electronic Data Reference Model (EDRM) (edrm.net), Collection Methods, http://edrm.net/wiki/index.php/Collection_-_Processes#Collection_Methods].

9.26[4] Forensic Data Capture Is Likely Necessary When Activity of User Is As Important As Content of Data. Manually copying files through a drag and drop process in Windows alters the directory-level metadata such as "Creation Date," "Last Access Date," and "Last Modification Date." So does using an "active data copy" software tool to collect information from a hard drive. Active data copy tools use the operating system's directory of data on the hard drive to automatically make a copy of the hard drive information.

Active data copy is a common and acceptable method of collecting ESI when the user's activity is not important to the issues in the case. However, active and manual data copying may be inappropriate for cases involving questions about the user's activity (for example, a trade secret case in which inappropriate copying of ESI is alleged), because both active and manual data copying alter directory-level metadata.

Example:

In *Covad Communs Co. v. Revonet, Inc.* (DDC 2009) 258 FRD 5, the issue was whether defendant had improperly accessed a database. The court allowed inspection and imaging of the database and its metadata regarding access because the issue of access was at the "heart of the case."

Forensic data capture techniques copy the information on a media asset (such as hard drive) bit by bit, without relying on the hard drive's internal indexing system. They create an "image" of the hard drive without altering the directory-level metadata. However, they are highly detailed and generally require a trained forensic specialist who is qualified to perform the task and can testify in court concerning the adequacy and reliability of the process.

9.26[5] Forensic Data Capture Is Likely to Be Necessary When Concerns Regarding Destruction of Data May Be Raised. Data residing on a computer hard drive ordinarily is not removed from the drive when the user deletes it. Rather, the computer's indexing system simply recognizes the hard drive sectors to which the data was assigned as once again available for new data. The data is still on the hard drive until the computer's indexing system assigns new data to those sectors.

Non-forensic data capture techniques rely upon the computer's indexing system to determine what data is available to be copied. They also alter directory-level metadata. In contrast, forensic data capture techniques copy the information on a media asset (such as hard drive) bit by bit, without relying on the hard drive's internal indexing system. When questions of data destruction are likely to be at issue in the case, forensic data capture techniques are appropriate.



Cross Reference:

Discussion of data storage, see *Ch. 1, Understanding Electronic Evidence, 1.18, 1.19.*



151 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
V. PERFORMING AND DOCUMENTING A DILIGENT SEARCH FOR RESPONSIVE ESI

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.27

AUTHOR: Ernst Halperin

9.27 If Risk of Intentional Destruction Exists, Court May Order Collection and Preservation of ESI by Neutral Expert.

Occasionally a court may order collection and preservation of ESI by a neutral expert. This tends to occur in cases in which there is already some indication of malfeasance by a party, most commonly in cases involving allegations of trade secret theft.

Example:

In *Dodge, Warren & Peters Ins. Services, Inc. v. Riley* (2003) 105 CA4th 1414, 1417-1418, 130 CR2d 385, the defendants had left their insurance brokerage agency to start a new one. Before leaving, they took photocopies of thousands of paper documents and copied most of the agency's computer files onto disks for later use at the new agency. The trial court issued a preliminary injunction requiring the preservation of electronic evidence by prohibiting defendants from destroying, deleting, or secreting from discovery any of their electronic storage media and by requiring them to allow a court-appointed expert to copy all of it, including computer hard drives and discs, to recover lost or deleted files and to perform automated searches of that evidence under guidelines agreed to by the parties or established by the court. The injunction was affirmed on appeal.

A request for appointment of a neutral expert to image data will usually be styled as a request for temporary restraining order and/or preliminary injunction. The party requesting the appointment of the neutral expert will need to show that [*Dodge, Warren & Peters Ins. Services, Inc. v. Riley* (2008) 105 CA4th 1414, 1417-1418, 130 CR2d 385] :

- The search to be conducted by the neutral expert is likely to result in obtaining discoverable evidence;
- The party requesting the collection by a neutral expert could irretrievably lose evidence that otherwise would have been available to it; and
- The harm from the potential loss of evidence outweighs the harm to the opposing party from granting the request.

**Strategic Point:**

The party requesting appointment of a neutral expert increases its likelihood of success if the burden on the responding party will be as low as possible. For example, the requesting party may reduce the burden by doing the following:

- Seeking to have the ESI copied in the opposing party's presence and after working hours so as to not interrupt its ability to conduct business.
- Showing that no damage to or loss of information would result from the copying.
- Providing that the copied material would be unavailable to anyone except upon agreement of the parties or order of the court.
- Agreeing that the reasonable cost to the opposing party to review the copied files for irrelevant and privileged documents will be borne by the party requesting the order, subject to reallocation by the trial court [*see Dodge, Warren & Peters Ins. Services, Inc. v. Riley* (2003) 105 CA4th 1414, 1421, 130 CR2d 385] .

**Cross References:**

Appointment of neutral expert, see 9.27.

Obtaining injunction against destruction of ESI, see Ch. 7, Obtaining Injunction to Protect Against Destruction of Electronic Evidence Pending Discovery.



152 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

V. PERFORMING AND DOCUMENTING A DILIGENT SEARCH FOR RESPONSIVE ESI

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.28

AUTHOR: Ernst Halperin

9.28 Narrowing Volume of Data to Review by Carefully Targeting and Limiting Media Assets to Be Harvested.

9.28[1] ESI Is Too Voluminous to Collect Indiscriminately. The great advantage of ESI--the ability to store large amounts of data--is also its greatest disadvantage when it comes to document collection for discovery. A simple CD-ROM can hold up to 70,000 pages of data. An 8-gigabyte USB thumb drive can hold 800,000 pages of data, or about 320 bankers' boxes. An individual user's laptop will often have a hard drive with a capacity of more than 100 gigabytes. Given these numbers, it is easy to see that indiscriminate collection of ESI from potential witnesses could easily overwhelm the ability of even the largest law firm to review all of the data collected.

The most efficient way to minimize the data to review is to limit the amount of data collected in the first place. However, the decision not to collect ESI must be done in a systematic, reasoned manner that will be defensible if challenged by the party that propounded the demand for production. A thorough understanding of the case issues, the client's organization and data systems, the role of key witnesses, and the data formats commonly used by the witnesses is indispensable in making defensible decisions.

9.28[2] Limiting Number of Witnesses Whose ESI Will Be Collected Limits Volume of ESI to Review. The first step in limiting the volume of data collected is to limit the number of witnesses whose ESI will be harvested for review. During the identification stage of the document collection process, it is important to carefully review the interviews of potential witnesses, in order to determine whether, in light of the issues in the case, and the witnesses' knowledge, their ESI should even be gathered for searching and processing. A balance must be struck between the need to do a comprehensive search for ESI and the need to do it in a cost-effective manner.



Strategic Point:

Counsel should consider the following questions:

- Which players in the dispute really matter?

- Is there a reasoned way of eliminating from the scope of the litigation witnesses who may have some information, but are nevertheless not key witnesses because they did not have the authority to make decisions, or only had limited information?

Example:

Assume that in a suit for breach of a merger agreement the defendant claims it was justified in terminating the merger because a material adverse effect on the plaintiff's business had occurred, and propounds demands for production demanding all communications regarding the plaintiff company's business performance. Plaintiff could object to the demand on the ground that it is unduly burdensome, and state it will produce responsive information only from the heads of the company's operating divisions. These are the witnesses who would have the aggregated information on the key question in the litigation--whether the company's business suffered a material adverse effect. Although employees further down the corporate hierarchy would also have some information about the performance of the divisions in which they work, the aggregated information in the possession of the main decision-makers more directly answers the key question and is much less voluminous.

9.28[3] Volume of ESI Can Be Further Reduced by Examining Whether Certain Types of Data Can Be Excluded. Another fruitful way to limit the data collected is to consider whether certain types of data can be excluded as irrelevant, duplicative, or not reasonably accessible in light of the issues in the case. The documents relevant to any particular litigation will most often be a small subset of the entire ESI located on the media assets of any particular custodian. Targeting the relevant documents by thoroughly understanding the case issues, and understanding how the individual document custodians organize their information, will allow counsel to make an informed, defensible selection of portions of the custodians' media assets most likely to contain potentially relevant documents.

9.28[4] Collecting a Defined Subset of Any Given Particular Data Type May Be Warranted. A third avenue is to limit, within a particular data type, the data to be searched.

Example:

In a dispute about a consultant's performance on a particular project, counsel's interviews with key witnesses reveal that they organize their e-mails into folders associated with individual client projects. The interviews also reveal that the employees are diligent about filing the e-mails into the particular project folders. Counsel's observation of their Outlook inboxes confirms their diligence. The inboxes rarely have more than a handful of e-mails in them. Based upon this information, counsel could make a reasoned determination to only collect e-mails from the witnesses' Outlook folders associated with the particular project at issue in the litigation, instead of from each witness's entire Outlook mailbox.

**Warning:**

Like other methods of limiting collection, this method has risks and may require counsel to defend the methodology later and perhaps to go back again for a costly second collection. Looking at the in-box will not tell counsel how many e-mails were never filed. Moreover, unless a witness copies himself or herself on every sent e-mail, the sent files may be incomplete. In addition, custodians who maintain e-mail folders may nevertheless delete e-mails that are believed to be duplicative or unimportant, so collections may not be complete.

**Strategic Point:**

If possible, counsel should obtain an agreement from opposing counsel or a court order allowing this form of collection, and if not, collect more broadly and narrow it down later in review.

9.28[5] Data Collected Can Be Further Reduced by Date-Restricting the Information Collected. Counsel's

knowledge of the case will enable counsel to determine the relevant time periods for evidence. Date-restricting the ESI to eliminate data first created outside those time periods weeds out documents that are irrelevant.

9.28[6] Keyword and/or Conceptual Searching May Be Used to Limit ESI Collections. The collection of ESI might also be limited by using search software that collects only ESI that meets the search criteria. Such software, often installed on the client's computer network, allows counsel to analyze the data in place *before* the data is collected for final review and processing.

The search software used to collect data may go beyond keywords to involve newer "conceptual search" techniques. Conceptual search software uses special algorithms to group or cluster together search results based upon similarity of concepts in the data files, so users can quickly identify related files and eliminate groups of non-relevant files. Search software may also feature de-duplicating capabilities that allow the user to set the similarity threshold to trigger elimination of near-duplicates or duplicates from the resulting review set. The software can also provide the user with statistical data about search results to help in prioritizing preliminary case assessment review. At least one program graphically represents the flow of e-mail communications based on the sender and subject and analyzes their time scale to help legal teams understand how information moved between custodians.

Consider:

One purveyor of this type of software in the United States claims that a Fortune 100 company using its software was able to cull and filter a review-set of data by more than 90 percent, reducing the set from 60 gigabytes (approximately 6 million pages of documents, or 2,400 bankers' boxes) down to slightly over 1,000 documents [see "Product Brief --Aungate Investigator and ECA," published by Autonomy, Inc. on its website at www.autonomy.com].



Strategic Points:

- Counsel must be prepared to educate opposing counsel and the court in the soundness of the techniques used in connection with search software, in the event the propounding party challenges the decision to eliminate large volumes of data from review. Justifying search methodology will likely require expert testimony to explain to the court the theoretical underpinnings of the algorithmic techniques used by the software. However, the soundness of conceptual search grouping is already starting to become judicially accepted [see *Disability Rights Council of Greater Washington v. Washington Metropolitan Transit Authority* (DDC 2007) 242 FRD 139 ("I bring to the parties' attention recent scholarship that argues that concept searching, as opposed to keyword searching, is more efficient and more likely to produce the most comprehensive results")]. The search strategy and culling process itself will need to be well documented and logged so as to provide an evidentiary basis for the reasonableness of the choices made.

- Moreover, counsel should work closely with any ESI consultant retained, so that counsel can understand the technical limitations of the search software utilized. Most electronic discovery search efforts run against an index of words extracted from the source data. Counsel should understand how the particular discovery software goes about extracting words to create the index and whether certain types of files are ignored in the extraction process, and be prepared to test the program's capabilities against a known data set of documents to verify that its indexing capabilities will allow it to capture relevant documents [see Craig Ball, "Ball In Your Court: All Wet" (Law Technology News August 2009)].



Warning:

Counsel should continue to apply the maxim to "collect narrowly but preserve broadly." Although counsel may limit the e-mail folders collected from particular key witnesses, it may be prudent to ensure that their entire Outlook mailboxes are preserved. Key witness files that are not initially searched should still be preserved, as should the files of witnesses with potentially relevant information who are not included in the first round of data collection. Any data that is eliminated through preliminary keyword or concept searching utilizing early case assessment software should be preserved. Counsel needs to retain the ability to go back and search for additional potentially responsive information if the propounding party successfully challenges the collection effort as too narrow in scope.



153 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

VI. ANALYZING COLLECTED ESI TO NARROW SCOPE OF DATA TO BE REVIEWED FOR PRODUCTION

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.29

AUTHOR: Ernst Halperin

9.29 CHECKLIST: Analyzing Collected ESI to Narrow Scope of Data to Be Reviewed for Production.

☐ Develop an analysis plan.

Discussion:

See 9.31

☐ Apply de-duplication techniques to reduce volume of data.

Discussion:

See 9.32

☐ Develop systematic and defensible search term strategy to reduce review set to a manageable volume of documents, and, if possible, agree with opposing counsel on that strategy.

Discussion:

See 9.33

☐ Consider whether retaining expert assistance is appropriate.

Discussion:

See 9.34

☐ Develop appropriate queries for gathering ESI from databases.

Discussion:

See 9.35



154 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

VI. ANALYZING COLLECTED ESI TO NARROW SCOPE OF DATA TO BE REVIEWED FOR PRODUCTION

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.30

AUTHOR: Ernst Halperin

9.30 Options and Strategy.

The ESI collected by even the most well thought-out and narrow collection effort may remain too voluminous for attorneys to review each file. Further analysis is commonly necessary to reduce the data to a manageable volume that can be effectively reviewed given the issues in the case, the amount at stake, and the resources available to the client. The two main techniques for further data reduction involve automated culling of duplicate ESI, and the use of search term strategies to narrow the set of data to be reviewed. Very often, specialized software is utilized that allows counsel to apply these techniques.



155 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

VI. ANALYZING COLLECTED ESI TO NARROW SCOPE OF DATA TO BE REVIEWED FOR PRODUCTION

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.31

AUTHOR: Ernst Halperin

9.31 Developing an Analysis Plan.

Counsel should be prepared to develop a defensible plan for carrying out de-duplicating of data and narrowing the data through application of search strategies. The elements of such a plan should include, at a minimum:

- An analysis of whether de-duplication of data is appropriate given the issues of the case, and if so, what criteria are going to be applied to handle near-duplicates. Some data-analysis software allows users to set the similarity threshold for near-duplicates, and then tell the software whether to keep the near-duplicates for later review or to exclude the near-duplicates from the review set.
- Selection of a defensible set of search terms and strategy for applying the searches to the data set. The search term limitations must not be so narrow as to invite complaints that one's client has not performed a reasonable search, but must not be so broad that they leave the resulting data set unmanageably large.

Distinguish:

Search terms in this context are used to limit the data reviewed from that earlier collected. Search terms and/or conceptual search software can also be used to limit the amount of data that is collected from custodians in the first instance [see 9.28].

- A set of criteria for analyzing the effectiveness of the data reduction techniques in reducing the volume of materials to review while still capturing relevant information.

Consider:

Counsel who are unfamiliar with ESI, and whose clients do not have in-house expertise in applying data-reduction methods to large data sets may want to consider hiring an expert to help develop and implement the plan.



156 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

VI. ANALYZING COLLECTED ESI TO NARROW SCOPE OF DATA TO BE REVIEWED FOR PRODUCTION

*1-9 MB Practice Guide: CA E-Discovery and Evidence 9.32***AUTHOR:** Ernst Halperin**9.32 Applying De-Duplication Techniques to Reduce Volume of Data.**

E-discovery processing and review software (and services) commonly provide the user with the ability to identify exact duplicates of a file. De-duplication is usually performed by application of a mathematical algorithm in which a calculation is used to assign a unique value to the content of a file. Duplicates are identified and tracked by the software. One of the duplicates can be reviewed manually. The other duplicates can be either eliminated from the review set, or batch-processed so that all of the duplicates receive the same treatment as the single instance of the file which was manually reviewed.

Some software also allows for the identification of "near duplicates"--that is, files that are very similar but not identical. Often the user can set the similarity threshold for segregation of "near duplicates."

**Warning:**

Caution should be taken in developing a plan for treating near duplicates. Counsel must make a careful assessment of whether near duplicates are likely to contain important information for a case by virtue of the fact that they are almost, but not quite, the same as other files. For instance, two copies of a long e-mail may be near duplicates, the only difference being that one shows a blind carbon copy to a person not listed on the recipient list of the other copy of the e-mail. If a critical issue in a case is who knew information transmitted in the e-mail, counsel would not want to have set up a protocol for handling near-duplicates that would have excluded one of the copies from the review or production. A common agreement for de-duplication is that de-duplication will be performed *within* custodian data sets but not *across* custodian data sets.

Example:

If Tom Jones had five copies of a particular electronic file, only one is produced from Tom Jones, but if three other custodians also had the file, it will be produced four times, once for each of the custodians.

Duplicate handling techniques also may help speed privilege review of the documents by allowing all duplicate copies to be tagged with the same privilege decision once one copy is reviewed.

**Warning:**

If a file with duplicates is found to be relevant and producible, it is advisable nevertheless to produce copies of the file from each custodian who had possession of a copy. Alternatively, the production database should reflect each of the custodians who had copies of the document. If only one of the duplicates is produced, opposing counsel may convince a court that document custodians have committed spoliation.

Example:

In *Nursing Home Pension Fund v. Oracle Corporation* (ND Cal 2008) 254 FRD 559, the defendant corporation produced only 15 e-mails sent or received by its CEO from his own e-mail files, but produced more than 1,650 of his e-mails from the files of other company employees. The court reasoned that the corporation had failed to preserve e-mails from its CEO, and granted an adverse inference sanction against the defendant. The case serves as a caution that de-duplication should be utilized as a tool for limiting the amount of data to be reviewed, but counsel may find it advisable to produce all duplicates of the same document that were identified by the de-duplicating software.



157 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

VI. ANALYZING COLLECTED ESI TO NARROW SCOPE OF DATA TO BE REVIEWED FOR PRODUCTION

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.33

AUTHOR: Ernst Halperin

9.33 Developing Systematic and Defensible Search Term Strategy to Reduce Review Set to a Manageable Volume of Documents.

9.33[1] Agreeing With Opposing Counsel on a Search Strategy Is Likely to Be Most Cost Effective. If counsel is able to develop a good working relationship with opposing counsel on discovery issues, agreeing on a set of search terms and a strategy for implementing it is likely to be the most cost-effective way of proceeding. It will eliminate fights about whether or not the producing party's search strategy fulfills its duty to conduct a reasonable search.



Strategic Point:

Keyword searching is generally accepted as a method of identifying responsive documents and narrowing the data-set to a manageable volume.

However, it is not always possible to agree on search terms. Counsel propounding a demand for ESI has an incentive to push for search terms that are over-inclusive in order to increase the chance that responsive documents are not missed, especially since responding counsel's client bears the cost of eliminating the non-responsive documents through a manual review. Despite this incentive, if the lawyers have developed a decent working relationship, propounding counsel may be willing to accept more limited search terms. Propounding counsel's client is likely to be on the receiving end of a demand for ESI as well during the litigation.

9.33[2] Ad Hoc Searching Is Likely to Be Ruled Insufficient. If counsel cannot agree on a search term strategy, counsel for the producing party must be prepared to defend the adequacy of the chosen search term strategy. Courts are becoming less willing to accept ad hoc searches as sufficient.

Example:

In *William A. Gross Construction Associates, Inc. v. American Manufacturers Mutual Insurance Company* (SDNY 2004) 256 FRD 134, 134], the court admonished: "[t]his Opinion should serve as a wake-up call to the Bar in this District about the need for careful thought, quality control, testing, and cooperation with opposing counsel in designing search terms or 'keywords' to be used to produce e-mails

or other electronically stored information."

Producing counsel should be prepared to meet the following standards [see *William A. Gross Construction Associates, Inc. v. American Manufacturers Mutual Insurance Company* (SDNY 2004) 256 FRD 134, quoting *Victor Stanley, Inc. v. Creative Pipe, Inc.* (D Md 2008) 250 FRD 251, 260] :

- Selection of the appropriate search and information retrieval technique requires careful advance planning by persons qualified to design effective search methodology.
- The implementation of the methodology selected should be tested for quality assurance.
- The party selecting the methodology must be prepared to explain the rationale for the method chosen to the court.
- The producing party must demonstrate that the methodology is appropriate for the task.
- The producing party must show that it properly implemented the methodology.

9.33[3] Carefully Crafted Search Strategy Allows Counsel to Demonstrate to Opposing Counsel and Court That Strategy Is Appropriate. A search strategy may involve just key word searching, or it can also involve conceptual search to identify related concepts (for example, the concepts of pricing and market might be identified as related to the concept of antitrust) [see 9.28[6] regarding use of conceptual search software in collecting documents]. Whichever technique is used, counsel must be prepared to defend the search strategy chosen by explaining the rationale for the method, and demonstrating that it is appropriate for the task. The strategy should employ some form of sampling or results testing, to ensure that the search strategy is finding responsive documents. A basic strategy could include [see "The Skeptical Searcher, or, How to Give Up the Full Review and Discover What Matters" (Daticon EED 2004, available at http://www.daticon-eed.com/about_IntheNews.htm)]:

- Using search terms developed from client interviews, key documents, lists of names and e-mail addresses, paper productions, company organizational charts and glossaries, and possibly from conceptual search technology.
- Running a test search, and reviewing the results by search term or custodian to determine whether the results fall in line with what one would expect, given what counsel knows about the case, the witnesses, and the data sources.
- Reviewing samples of the data collection when no hits were found, among the data of witnesses who otherwise have responsive data. This can tell counsel whether the search parameters are failing to catch relevant documents.
- Revising and re-testing the search terms to document the testing and results, to be able to prove to the court that a rational procedure has been followed.
- Employing separate sets of search terms to help find privileged data.

Reviewing the test results can be done by looking at the results of a test run, and then iteratively building the search list by adding terms. This procedure is very defensible, but can be time consuming. An alternative is to use statistical reports in evaluating the search results to determine whether "hits" are occurring in the data of the custodians one would expect, given what counsel knows about the witnesses and the case issues.



158 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

VI. ANALYZING COLLECTED ESI TO NARROW SCOPE OF DATA TO BE REVIEWED FOR PRODUCTION

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.34

AUTHOR: Ernst Halperin

9.34 Counsel Should Consider Retaining Expert Assistance If Case Is Hotly Contested or Involves a Large Volume of Data in a Variety of Formats.

Being able to design an effective search strategy may be outside counsel's core competency. An expert in search theory and practice can also be useful in demonstrating to the court that the search strategy is adequate for the task. If the producing party's search strategy is challenged, the court may want expert guidance on what is reasonable, which may require the application of statistical analysis techniques.

Consider:

At least one federal court has opined that expert testimony is required, at least in complex cases [*see* *United States v. O'Keefe* (DDC 2008) 537 F Supp2d 14, 24]. Although no California case has gone so far as to require expert opinion, it would not be surprising to see more courts accept that view, especially if concept-based automated search techniques employing sophisticated algorithms are used in reducing the volume of data for manual review.



159 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information

VI. ANALYZING COLLECTED ESI TO NARROW SCOPE OF DATA TO BE REVIEWED FOR PRODUCTION

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.35

AUTHOR: Ernst Halperin

9.35 Developing Appropriate Queries for Gathering ESI From Databases.

In gathering and producing ESI from a database, counsel should understand and distinguish between whether the actual raw data is needed, or whether reports created from the raw data are needed.

A database is a collection of mutually related data or information stored in computer record fields. Databases may track key business information that may be useful in discovery, such as employee information, job classifications, records of sales, and other relevant data. The information in databases is often structured and customized in ways particular to an organization. For example, a business database might track sales in one table, customer names in a second table, and customer addresses in a third table. The tables of raw data from the database will be useful to the receiving party only if the data structure and information storage protocols are completely understood so that the receiving party (or its expert) may load the raw data into a database and run its own queries. This raw data from the database will usually be transferred by text load files that indicate the start and end of fields and records.

Alternatively or in addition, the receiving party may seek a report of the underlying data in response to a database query. Thus, if the information sought in the dispute is the names and addresses of customers in California who bought an item in July 2009, a report generated from a query done by the producing party may be more useful than the underlying raw data.

A business client is likely to have considerable expertise within its organization in querying its operational structured data systems. Counsel's preliminary analysis of the case and meetings with the client's information technology personnel should have already identified those structured data systems that are likely to have information responsive to demands for production.

Whether the ESI produced will be in the form of raw data tables or reports, counsel should work with the client's information technology personnel to develop database queries that will produce the required information. Counsel may also need to meet and confer with opposing counsel to educate opposing counsel about what data is maintained and in what form it may be produced. When developing the queries, counsel should ensure that the client's IT personnel validate the queries by running them on known data-sets to determine if they produce the expected results.

**Strategic Point:**

Counsel should keep in mind that extensive steps to query and produce data from a database might be considered "translation" from a "data compilation" using "detection devices," and therefore enable the producing party to shift the reasonable costs to the demanding party [see *CCP* §§ 1985.8(g) (cost-shifting for translation for subpoena); 2031.280(e) (cost-shifting for translation done by a party)].

**Cross Reference:**

Discussion of cost-shifting provisions of Electronic Discovery Act, see *Ch. 4, Planning E-Discovery*, 4.08[4][b].



160 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
VII. REVIEWING FOR RESPONSIVENESS AND PRIVILEGE

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.36

AUTHOR: Ernst Halperin

9.36 CHECKLIST: Reviewing for Responsiveness and Privilege.

- ☐ Choose the review methodology and software platform.

Discussion:

See 9.38

- ☐ Evaluate whether to perform case assessment concurrently with review.

Discussion:

See 9.39

- ☐ Develop an effective review procedure.

Discussion:

See 9.40

- ☐ Educate review team about case and privilege issues.

Discussion:

See 9.41

- ☐ Identify and segregate privileged information.

Discussion:

See 9.42-9.43

- ☐ Review the remaining documents.

Discussion:

See 9.44

- ☐ Prepare privilege log.

Discussion:

See 9.45



161 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
VII. REVIEWING FOR RESPONSIVENESS AND PRIVILEGE

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.37

AUTHOR: Ernst Halperin

9.37 Options and Strategies.

Manual review for privilege and responsiveness is the most expensive component of producing ESI in response to a discovery demand. Counsel must choose the review methodology that is most appropriate for the needs of the case, considering the volume of ESI to be reviewed, the case budget, and the time for production. Counsel also must make a determination of whether to perform case assessment tasks concurrently with the review for responsiveness and privilege. A large proportion of privileged documents can be identified and processed together through the use of key word searching. However, the remaining documents must also be checked for privilege as well [*see, e.g., Rhoads Indus. v. Bldg. Materials Corp. of Am. (ED Pa 2008) 254 FRD 216* (party that relied on inadequate search terms and methodology failed to catch more than 800 privileged documents in its review)]. Grouping the potentially privileged documents speeds up the review process.



162 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
VII. REVIEWING FOR RESPONSIVENESS AND PRIVILEGE

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.38

AUTHOR: Ernst Halperin

9.38 Review Methodology and Software Depend on Budget and Needs of Case.

9.38[1] Manual Paper-Based Review May Be Appropriate in Limited Circumstances Involving Very Small Datasets. When a small data set is involved, manual paper-based review may be appropriate. This most commonly happens in very small organizations when the client has self-selected the potentially relevant documents, or on a smaller matter when opposing counsel requests production of the documents in paper format.

Manual paper-based review has the disadvantage that all of the metadata is lost when the documents are printed to paper. Moreover, information that is located in "hidden" columns on spreadsheets will be lost if the spreadsheets are printed from their native applications. Formulas in spreadsheets will also be lost.

Consider--Production Cost for Paper-Based Review:

The cost of preparing ESI for paper-based review is not necessarily lower than preparing ESI to be reviewed in near-native or native format with database or specialized review software. The price of printing out a review copy set, Bates stamping, and then copying the documents selected for production is often more expensive than the cost of creating a set of image files in the two most common formats (TIFF and PDF), and populating a database load file with the metadata. Production of data in TIFF or PDF format is usually done on CD-ROM, and the cost of making a production CD is small relative to the costs of printing many documents.

The cost of attorney and paralegal time for performing a paper-based review also is likely to be higher than for reviewing the information in TIFF, PDF, or native-file format using a review platform. It also can be much harder to keep track of documents once they have been printed. Document tracking must be performed manually, and basic privilege log data such as document date, sender, and recipient has to be entered manually. If the reviewer is also issue coding the documents, indexes of the documents by issue-code must be created manually. In contrast, most software used for document review allows users to track what has and has not been reviewed, creates indexes of the documents by issue code, and populates privilege log fields from the file metadata. These differences often make paper-based review more expensive overall.



Warning--Paper May Not Always Be "Reasonably Usable" Form.

The Electronic Discovery Act requires a producing party to produce ESI in a form that is "reasonably usable" [see *CCP* § 2031.280(d)(1)]. A party making a demand for production may also specify the form in which each type of ESI will be produced. [*CCP* § 2031.030(a)(2)]. If the party making the demand has not specified paper and will not agree to production on paper, counsel probably should not produce the information on paper. Opposing counsel would have a good chance of successfully arguing to the court that the producing party had not fulfilled its obligation to produce ESI in a "reasonably usable" form, especially if it could demonstrate that metadata or hidden spreadsheet columns would contain information relevant to the issues in the case.

9.38[2] Systems That Rely on Conversion of Documents to TIFF or PDF Format Prior to Review Have Commonly Been Used for Medium-Sized Cases.

9.38[2][a] Electronic Files Are Converted in Image Files. The most common method of document review for medium-sized data sets has been to first convert the electronic data files into image files. The two major image formats are Tagged Image File Format ("TIFF") and Portable Document Format ("PDF"). Next, metadata and the file text are extracted from the native files and loaded into a review platform such as Concordance or Summation.

9.38[2][b] Attorney Can Review Image Files Without Danger of Altering Them. Using a review platform, the reviewing attorney can see the TIFF or PDF image of the file while looking at the database entry showing the metadata and file text. Some of the systems also link a copy of the native file in read-only mode to the database record to give the reviewing attorney the choice of looking at the original file instead of a TIFF or PDF image. Clicking on the link opens the file using the application (such as Word, Excel, or PowerPoint) associated with the file type.

Since the native file is in "read only" mode, the reviewing attorney cannot alter potentially critical metadata such as "last modified date" by inadvertently saving the file during review. Some vendors offer a generic viewer that renders the native-format file into HTML when the reviewing attorney clicks the link. This allows a reviewing attorney to view the file without having to have the original application on the reviewing computer.

9.38[2][c] E-Mails Are Converted Into HTML or Plain Text Files. E-mails are handled slightly differently than other types of files. Most vendors' systems convert the e-mail files into HTML or plain text format, while maintaining attachments in native file format in read-only mode.

9.38[2][d] User Categorizes Documents. Typically the reviewing platforms allow the user to designate documents as responsive, nonresponsive or privileged by checking boxes on the software's user interface. The platform also typically allows reviewing attorneys to issue-code the documents using the same box-checking method. Most of the programs have a graphical interface that allows the user to redact portions of the viewed image of a file.

9.38[2][e] Cost of Conversion Is a Disadvantage. There are disadvantages to systems that rely upon conversion of the files to TIFF or PDF format for review. The major disadvantage is cost. All of the files are converted to TIFF or PDF format before review, so the client ends up paying for the cost to convert nonresponsive documents that ultimately will not be produced.

9.38[2][f] Difficulty of Conversion Can Be a Disadvantage. The second disadvantage is the difficulty of converting certain document types into readable TIFF files.

Excel spreadsheets are notoriously problematic. A formatted spreadsheet with hidden columns that is two or three pages long when viewed from within the Excel application can easily expand to 30 or 40 pages when converted to TIFF format, depending upon how the conversion is accomplished. Most vendor software does not preserve the spreadsheet formatting when converting the files. Instead, all of the rows and columns within the "four corners" of the data are printed onto TIFF images. Sometimes the conversion creates dozens of pages of blank spreadsheet rows and columns in

between TIFF images with numbers on them. The information value of a spreadsheet derives both from the numbers themselves, and from their positioning relative to each other. By changing the manner in which that positioning is displayed, the TIFF conversion process can often affect the utility of the spreadsheet.

One way of handling the conversion problem with Excel spreadsheets is to produce Excel files in native format. In the event the original spreadsheet contains some privileged information requiring redaction, the review copy of the spreadsheet in native file format is unlocked, and the privileged information replaced in the native file with the word "REDACTED." This manual workaround alters the review copy of the spreadsheet itself, and changes the spreadsheet's file-level metadata. If this technique is utilized, counsel should disclose the technique to the demanding party's attorney, and document the disclosure in written correspondence accompanying the production. Counsel should also ensure that an un-redacted original of the Excel file is maintained.

Another way of handling the difficulty of converting Excel files to readable TIFFs is to produce the TIFFs, and have an agreement with opposing counsel that in the event that important spreadsheets are difficult to understand and work with in TIFF, a native copy will be produced as well (Note that this agreement is necessary because the default rule is that ESI need be produced only in a single format [*CCP* § 2031.280(d)]).

9.38[3] Some Vendors Offer Native File Review With TIFF Conversion on Demand. Native file review with TIFF conversion on demand by the user allows the client to avoid the cost of conversion of the entire review dataset to TIFF or PDF format.

Example:

Some vendors charge 8 to 15 cents per page for TIFF conversion. One gigabyte of data equals approximately 75,000 to 80,000 pages. For a 5-gigabyte data set in which 30 percent of the documents are either nonresponsive or privileged, native file review could save the cost of converting approximately 112,500 pages of TIFF files. At 8 cents to 15 cents per page, the savings from native file review would be between \$9,000 and nearly \$17,000.

A disadvantage of native-file review can be that click-through times will be slower than for review in TIFF or PDF format, especially when the reviewing platform relies upon the native application to open the files.



Strategic Point:

If the data is being reviewed on a platform that offers native file review, counsel should ensure that the reviewers examine hidden rows and hidden columns, headers, footers, and any tracked changes.

9.38[4] Online Hosted Review Systems Allow Geographically Dispersed Teams to Effectively Review Large Amounts of Data While Maintaining Appropriate Audit Trail of Review Activities. For very large productions in which dozens, or possibly, hundreds of reviewers will need to work with the ESI, vendors offer online hosted review platforms. When choosing among vendors, it is important to understand the process control and auditing features they provide so that counsel can plan and track the review properly.



163 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
VII. REVIEWING FOR RESPONSIVENESS AND PRIVILEGE

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.39

AUTHOR: Ernst Halperin

9.39 Counsel Should Evaluate Whether to Perform Case Assessment Concurrently With Review.

Depending upon the volume of data to review and production deadlines, counsel may want to incorporate some form of case assessment into the review process. This can be as simple as having reviewing attorneys flag "key" documents as they review documents for responsiveness to the document demand and for privilege. Somewhat more complicated and time consuming is to label reviewed documents with "issue codes." Even more time consuming, some review platforms allow the user to export a key document into case assessment software during the review, and draft a note about the fact proven by the document directly in the case assessment software. Most recently, conceptual searching techniques are allowing counsel to perform early case assessment at a macro level and to identify key documents and relationships by reviewing similar documents that have been clustered together by the software.

There is a tradeoff, however, between efficiency and speed of review: the more complex the case assessment tasks performed by the reviewers, the slower the review. When the case involves large data sets with tight production deadlines, there simply may not be enough time to do more than review for relevance and privilege.

Counsel faced with a very large data set may have already considered using conceptual search tools to cull the information to be collected for review. Conceptual search software can also be applied during the manual review process to aid in case assessment in cases with smaller datasets as well. In a standard review process, the reviewers work through the data in a linear fashion--performing the review record by record in the order that the records are loaded into the review database. Very often that order is the same order in which the files were collected, with files organized by custodian. Conceptual search software visually clusters documents together based upon keywords, or algorithmically derived similarity of concepts. This clustering can help users identify key documents more quickly than when documents are not clustered because key documents containing similar concepts are clustered together.



Cross Reference:

Discussion of conceptual search software, 9.28[6].



164 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
VII. REVIEWING FOR RESPONSIVENESS AND PRIVILEGE

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.40

AUTHOR: Ernst Halperin

9.40 Components of an Effective Review Procedure.

A large document review requires systematic planning and project management to keep it on track. The components of the plan should include, at a minimum:

- Choose a review platform.
- Decide what, if any, case assessment tasks will be performed by the review team, and design any issue codes and privilege codes that the team will use.
- Educate the project team about the case and privilege issues.
- Set interim deadlines and track the progress of the team.
- Carefully review privilege logs developed by the team.
- Perform quality control on the reviewed documents to ensure the team is performing according to plan.



165 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
VII. REVIEWING FOR RESPONSIVENESS AND PRIVILEGE

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.41

AUTHOR: Ernst Halperin

9.41 Educating Review Team About Case and Privilege Issues.

9.41[1] Review Team Members Should Be Thoroughly Educated About Case. In order to determine whether the documents they are reviewing are responsive to the demand for production, the reviewing attorneys must, of course, be thoroughly familiar with the document demand. However, they should also review the producing party's written responses to the demands for production in order to understand what categories of documents are likely to contain privileged materials, and what kinds of documents will not be produced.

Ideally, the review team should also have a thorough understanding of the case as a whole, especially if the team is going to be performing case assessment duties. All members of the team should review the pleadings and briefs from any demurrers. It is also extremely helpful to inculcate the reviewing attorneys in the theory of the case. They will be better equipped to identify key documents, and to perform issue coding if that is required.

9.41[2] Reviewing Attorneys Must Understand Relationships Between In-House Counsel, Outside Counsel, and Attorneys Not Affiliated With Client. Privilege review is an important part of the document review process. A waiver of attorney-client privilege should never occur unless purposefully done for strategic reasons (for instance, as part of an advice of counsel defense).

Reviewing attorneys must understand the role of every lawyer and law firm mentioned in the data being reviewed in order to properly segregate privileged documents. The review team should be given a list of all of these attorneys, with a synopsis of their contribution or role in the matter for which they were retained.



166 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
VII. REVIEWING FOR RESPONSIVENESS AND PRIVILEGE

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.42

AUTHOR: Ernst Halperin

9.42 Attorney-Client Privilege and Attorney Work Product Privileges Are Easily Waived.

9.42[1] Voluntary Production of Privileged Material Waives the Privilege. The attorney-client privilege is waived by a voluntary disclosure of the communication [*Evid Code* § 912(a)]. This has led in the past to serious disputes about whether a disclosure was inadvertent or not. The risks of waiver are high, both for the client, and for the attorney. With the increase in volume of ESI, the risk of producing large amounts of privileged materials without meaning to increases dramatically.

9.42[2] CCP § 2031.285 Provides a Method for Party Inadvertently Producing Privileged Information to Claw It Back. If ESI ends up in a production to the other side, the Electronic Discovery Act provides a mechanism for counsel to notify the lawyer for the receiving party, and prevents the other counsel from using the material until the court has had the opportunity to determine whether the material is, indeed, privileged [*CCP* § 2031.285(b), (c)(2)]. However, the claim of privilege can still be contested, including the question of whether the disclosure was so careless that the privilege should be considered waived.

Example--No Waiver by Inadvertent Production:

The court found no waiver when three pages of privileged e-mails were inadvertently produced in a 40,000 page document production and the supervising attorney had implemented a formal privilege review protocol for the two document review paralegals with 16 and 17 years of experience [*Coburn Group, LLC v. Whitecap Investors LLC* (ED ILL 2009) 640 F Supp2d 1032] .

➤ Cross Reference:

Discussion of method under the Electronic Discovery Act for asserting claims of privilege after inadvertent production, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference*, 5.19[6].



167 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
VII. REVIEWING FOR RESPONSIVENESS AND PRIVILEGE

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.43

AUTHOR: Ernst Halperin

9.43 Identifying and Segregating Privileged Information.

9.43[1] Stipulating With Opposing Counsel That ESI Belonging to In-House Counsel Need Not Be Searched or Produced Can Save Significant Resources. ESI associated with in-house counsel is likely to contain large amounts of privileged information, although some of it may be responsive to a demand for production. The most efficient way to deal with this problem is to attempt to stipulate with opposing counsel that the responding party need not search for responsive documents from the files of in-house counsel. Opposing counsel will have an incentive to do this because he or she will want to avoid the same issue when responding to a demand for production. In some types of cases, such as breach of contract disputes when in-house counsel was heavily involved in the negotiation of the contract, it may not be possible to reach such an agreement.

9.43[2] Appropriate Search Terms Can Help Identify Privileged Documents. Searches should be run on the names of all of the known attorneys for the client to identify a subset of the documents likely to contain privileged information. Counsel should remember to include the names of outside counsel and their firms. Common misspellings of the names should also be included in the search terms to cast as broad a net as possible. The resulting documents can be group tagged as "provisionally privileged--do not produce."

The provisionally privileged documents will need to be manually reviewed to determine if, in fact, they are actually privileged, or if they are not by virtue of having been communications with people outside of the privilege.



Warning:

Do not rely upon the searches alone to identify privileged documents. All documents from the review set should be checked for privilege, not just the "provisionally privileged" documents identified by the searches [see *Victor Stanley Inc. v. Creative Pipe (D Md 2008) 250 FRD 251* (privilege held to be waived when 165 documents inadvertently were produced due to failure of search strategy to catch the documents)].



168 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
VII. REVIEWING FOR RESPONSIVENESS AND PRIVILEGE

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.44

AUTHOR: Ernst Halperin

9.44 Reviewing Documents Segregated As "Provisionally Privileged"

9.44[1] Holding Back Entire Documents That Are Privileged. If the entire document is privileged, the reviewing platform should provide the capability for counsel to designate the documents as "privileged--do not produce." In a common reviewing database such as Concordance, this can be done with check boxes that the reviewing attorney clicks with a mouse.

The reviewing platform should be configured to allow the attorney performing the review to immediately create a draft privilege log entry explaining the basis of the privilege, while the document is fresh in his or her mind.

9.44[2] If Only Part of Document Is Privileged, Reviewing Platforms Should Provide Method to Specify Text to Be Redacted From Final Produced Image. Many documents will need to be redacted prior to production, and the reasons for the redaction logged into the privilege log. Reviewing platforms commonly provide a method for accomplishing this task. If documents are reviewed in TIFF or PDF format, the software commonly provides a graphical means for the reviewer to highlight and black out the privileged portions of the document. As with entirely privileged documents, the reviewing software can be set up with check-boxes to indicate redacted records to be produced with the privileged materials obscured.



Warning:

Note that when using a review platform such as Concordance, covering the privileged material on the graphic image of the document will not remove the privileged material from the extracted document text in the database. If counsel has agreed to exchange the extracted document text as part of the load file of metadata accompanying a set of documents in TIFF format, the privileged text will need to be removed from the load file before production.



Warning:

In most cases, the graphical interfaces in review platforms *do not* actually eliminate the text on the TIFF or PDF that the reviewing attorney has highlighted and blacked out (although newer versions of Adobe Acrobat Pro do eliminate the underlying text). Typically, the programs "redact" text by electronically

pasting an opaque layer over the highlighted portion of the TIFF or PDF document. The privileged information remains below the opaque layer. With both types of files there are a number of techniques that allow anybody to view the underlying information.

Both TIFF and PDF files *must* undergo further processing before production. With TIFF files, a new TIFF is burned in a process that is analogous to photocopying a paper document that has redacting tape placed over privileged text. With PDF files, the current version of Adobe Acrobat 9 Pro now incorporates a redaction tool that allows the user to remove all redacted text from the image and the underlying text. The process requires two steps, the first consisting of marking the text for redaction with a tool that allows the user to cover the text with an opaque rectangle, and the second being removing the underlying text and re-saving the document. If the user fails to perform the second step, the "redacted" text will still be part of the PDF file.

A reasonable attorney would not even think of producing an original document with redacting tape on it instead of a photocopy of the redacted document. Yet there have been a number of instances in which the electronic equivalent has occurred when lawyers did not understand the basics of the technology and allowed improperly processed PDFs to be produced or electronically filed with courts [see, e.g., Malan, Douglas S., "GE Suffers a Redacting Disaster," The Connecticut Law Tribune, May 28, 2008].



Examples:

Former Illinois Governor Rod Blagojevich's defense team electronically filed a motion for a court order to issue a trial subpoena to compel President Obama to testify at Governor Blagojevich's criminal trial. The defense team filed a PDF of the motion that still contained the redacted text beneath an opaque cover layer [see April 28, 2010 Chicago Lawyer Lextek Report blog entry "Redaction Snafu Offers Bad Example of eDiscovery Practice" at <http://lextekreport.com/2010/04/28/blago-redaction-snafu-offers-bad-example-of-ediscovery-practice/>].

This problem is not unique to lawyers. In one reported instance, the Transportation Safety Administration posted an improperly redacted security manual on its website without scrubbing the PDF's hidden text beneath the opaque layers [see Hsu & Johnson, *TSA Accidentally Reveals Airport Security Secrets*, Washington Post 12/9/2009].

9.44[3] Listing Individual Privileges As Separate Issue Codes Can Speed Compilation and Editing of Privilege Log. The reviewing software should be set up with different check boxes for individual privileges (e.g., Attorney Work Product, Attorney-Client, etc.). The reviewing attorney checks as many of the privileges that apply, and then writes a short entry directly into the reviewing software database record for the file, describing the basis for the privilege assertion. This technique speeds compilation and editing of the privilege log because all of the information about the privilege assertion is already associated with the file record.



Strategic Point:

CCP § 2031.240(b)(2) only requires a responding party to state objections in its response. Failure to provide a privilege log to the party propounding a demand for production does not waive privilege under state court practice [*Best Products v. Superior Ct. (2004) 119 CA4th 1181, 1188, 15 CR3d 154* (privilege log is not required with response, and not relevant until after the propounding party challenges a claim of privilege)]. Nevertheless, it is a good idea to prepare one because a court can ask for specifics on a motion to compel as to the basis for asserting a privilege.

 Cross References:

Discussion of privilege logs, see 9.46.

Sample privilege log entry, see 9.46



169 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
VII. REVIEWING FOR RESPONSIVENESS AND PRIVILEGE

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.45

AUTHOR: Ernst Halperin

9.45 Reviewing Remaining Documents.

9.45[1] Remaining Documents Must Still Be Checked for Privilege. After segregating the potentially privileged documents through keyword searching for attorneys' names, counsel may be tempted not to carefully check the remaining documents for privilege when performing the review for responsiveness. That would be a mistake, since it assumes that the term search would be over-inclusive instead of under-inclusive, and would catch all of the potentially privileged documents. One does not want to risk a court ruling that counsel waived attorney-client privilege by not reviewing documents when there existed a risk that the key word search might not catch all of the privileged documents.

Example:

In *Rhoads Indus. v. Bldg. Materials Corp. of Am.* (ED Pa 2008) 254 FRD 216, privileged documents were inadvertently produced after an inadequate keyword search for privileged documents.



Cross Reference:

Identifying and Segregating Privileged Information, see 9.43

9.45[2] Issue Codes Should Be Established Based on Elements of Case Identified During Review of Pleadings, Demurrers, and Model Jury Instructions. If counsel has decided to have the review team issue code documents as they review for responsiveness and privilege, a set of issue codes will need to be established. The elements of the causes of action form the building blocks for a basic set of issue codes. Not every element in the cause of action should be listed as a code--only those that are likely to be contested. Otherwise, the issue code list becomes too unwieldy.

Example:

CACI instruction 303 gives the elements for breach of contract. To recover damages from the defendant for breach of contract, plaintiff must prove all of the following [*Judicial Council of California Civil Jury Instructions, CACI No. 303* (LexisNexis Matthew Bender)]:

1. That plaintiff and defendant entered into a contract;

2. That plaintiff did all, or substantially all, of the significant things that the contract required plaintiff to do, or that plaintiff was excused from doing those things;
3. That all conditions required by the contract for defendant's performance had occurred;
4. That defendant failed to do something that the contract required defendant to do; and
5. That plaintiff was harmed by that failure.

Suppose defendant has admitted that it entered into a contract to purchase ball bearings and that it did not pay for them. Defendant disputes that the plaintiff provided ball bearings that were within the specifications. Defendant argues that, in any event, the plaintiff was not harmed by the defendant's failure to pay because it was able to sell the bearings to another party for more money. A preliminary set of issue codes for the cause of action for breach of contract could be:

303(2) Conformance to specifications.

303(5) Harm to plaintiff.



170 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
VII. REVIEWING FOR RESPONSIVENESS AND PRIVILEGE

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.46

AUTHOR: Ernst Halperin**9.46 Preparing Privilege Log.**

The reviewers should prepare a list or "privilege log" of all documents for which a privilege is claimed in whole or in part. The purpose of a privilege log is to provide a specific factual description of documents in order to substantiate a claim of privilege [*Best Products v. Superior Ct. (2004) 119 CA4th 1181, 1188, 15 CR3d 154*]. The purpose of providing a specific factual description of documents is to permit a judicial evaluation of a claim of privilege [*Best Products v. Superior Ct. (2004) 119 CA4th 1181, 1188, 15 CR3d 154*].

The reviewing attorneys perform the first cut at the privilege log when they flag the individual privileges using the reviewing software platform, and draft a short entry describing the basis for the privilege in a field of the reviewing database. The draft privilege log can easily be created by exporting these fields and the metadata (such as from/to/cc/date/sender/recipient) of the ESI to fill out the appropriate fields of the privilege log.

**Strategic Point--Drafting Privilege Log Entries:**

The art of drafting a privilege log entry is to give enough information to establish the factual basis for the privilege without revealing a substantial portion of the substance of the communication.

Example:

Doc #	Date	From	§§ To	Description	Privilege Basis
2041	1/23/2009	John Smith, Esq.	Jane Doe	E-mail responding to request for legal ad- vice	Attorney-client; At- torney Work Product



171 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
VIII. PRODUCING DOCUMENTS TO THE DEMANDING PARTY

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.47

AUTHOR: Ernst Halperin

9.47 CHECKLIST: Producing Documents to the Demanding Party.

- ☐ Choose an appropriate format for production of ESI.

Discussion:

See 9.49-9.54

- ☐ Negotiate a realistic time for production of the ESI.

Discussion:

See 9.55

- ☐ Document each stage of the production.

Discussion:

See 9.67

Form:

See 9.60



172 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
VIII. PRODUCING DOCUMENTS TO THE DEMANDING PARTY

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.48

AUTHOR: Ernst Halperin

9.48 Options and Strategy.

Producing counsel has an obligation to produce ESI in a "reasonably usable" format. Although very small productions can be done on paper, one should not attempt to produce on paper without the opposing party's agreement. The most common format for production is an image file (TIFF or PDF), accompanied with a load file of the metadata that the parties have agreed will be exchanged. Negotiate realistic timelines for production that satisfies the desire of propounding counsel to get information quickly, while giving the producing party's attorneys adequate time to conduct a diligent search and review for responsiveness and privilege.



173 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
VIII. PRODUCING DOCUMENTS TO THE DEMANDING PARTY

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.49

AUTHOR: Ernst Halperin

9.49 Demanding Party May Specify Form of Production.

The Electronic Discovery Act provides that the party making the demand for production "may specify the form or forms in which each type of electronically stored information is to be produced" [CCP § 2031.030(a)(2)].



174 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
VIII. PRODUCING DOCUMENTS TO THE DEMANDING PARTY

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.50

AUTHOR: Ernst Halperin

9.50 Responding Party May State Form in Which It Intends to Produce ESI.

9.50[1] Responding Party Must Produce ESI in "Reasonably Usable" Form. Even if the demanding party has specified a form of production, the responding party can object to the specified form. An objecting party must state in its response the form in which it intends to produce each type of information [*CCP* § 2031.280(c)]. The responding party nonetheless has an obligation to produce the information in a form "that is reasonably usable" [*see CCP* § 2031.280(d)(1)]. If the demand for production does not specify a form, the responding party "shall produce the information in the form or forms in which it is ordinarily maintained or in a form that is reasonably usable" [*see CCP* § 2031.280(d)(1)].

Warning:

The option to produce in a "reasonably usable form" does not mean that a responding party is free to convert ESI from the form in which it is ordinarily maintained to a different form that makes it more difficult or burdensome for the requesting party to use the information efficiently in the litigation. If the responding party ordinarily maintains the information 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 [*AccessData Corp. v. ALSTE Techs. GmbH* (D Utah, Jan. 21, 2010) 2010 U.S. Dist. LEXIS 4566, *19 (D Utah, Jan. 21, 2010) (citing *Fed. R. Civ. P. 34(b)* Advisory Comm. Notes to 2006 Amendment)].

9.50[2] Initial Meet and Confer Should Have Addressed Production Format Issues. Ideally, disagreements about format will have been resolved before document request responses are due, because format of production is one of the topics for ESI meet and confer under *Rule 3.724(8)* [*see Cal Rules Ct, Rule 3.724(8)(B)* (parties must discuss the form or forms in which ESI will be produced during the mandatory meet and confer in advance of the initial case management conference)]. If disagreements nevertheless remain when ESI is to be produced, counsel may object to the requested format and produce in an alternate format. However, counsel should consider trying to meet and confer and reach an agreement before unilaterally providing ESI in an alternate format. An agreement as to the form of production will remove the chance of losing on a motion to compel and being required to produce again in the requested format.

Cross Reference:

Discussion of meet and confer requirements and strategy, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferring, and Case Management Conference, 5.14-5.21*.



175 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
VIII. PRODUCING DOCUMENTS TO THE DEMANDING PARTY

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.51

AUTHOR: Ernst Halperin

9.51 Paper Production Is Only Appropriate for Smallest Datasets or When Agreed Upon by Opposing Counsel.

Paper production used to be the most common form of production. It is a format familiar to all attorneys, and does not require advanced technological skills to accomplish. With the vast amount of ESI now being created in organizations, paper production has become impractical for all but the smallest productions. A production of 3 gigabytes of ESI is not uncommon in these days when computers routinely have hard drives holding more than 100 gigabytes. Depending upon the types of files contained, a 3-gigabyte production printed out on paper might require about 90 bankers' boxes to hold.

Moreover, paper production is not likely to be considered a "reasonably usable" form because it is not as searchable or sortable as the electronic form, and because it eliminates all of the metadata associated with ESI. This metadata can provide valuable evidence that is important to a contested issue in the case. Absent agreement of opposing counsel, producing documents in paper format is risky. If opposing counsel can show that the metadata is likely to have information important to a contested issue in the case, it will be hard to argue that a production format which strips away this important information is "reasonably usable."

Examples:

- In *Lombardo v. Broadway Stores (2002) 2002 Cal App Unpub LEXIS 4700, 1-2*, the destruction of the computerized form of records was sanctionable even though a printout existed.
- In *L.H. v. Schwarzenegger (CD Cal 2008) 2008 US Dist LEXIS 86829*, sanctions were imposed for producing non-sortable PDFs.
- In *3M Co. v. Kanbar (ND Cal 2007) 2007 US Dist LEXIS 45232*, a party that produced 170 boxes of paper was ordered to reproduce it in electronic format.



Cross References:

Discussion of hard copy production of ESI, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference, 5.19[3][b]*.

Privilege review of documents in paper format, see *9.38[1]*.



176 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
VIII. PRODUCING DOCUMENTS TO THE DEMANDING PARTY

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.52

AUTHOR: Ernst Halperin

9.52 Production in TIFF or PDF Format Accompanied by Load Table of Agreed-Upon Metadata Is Common.

9.52[1] Production of ESI in TIFF or PDF Format Allows Information to Be Easily Utilized in Connection With Case Management Software. The major software programs used for case and document management allow information in the two most common formats (TIFF and PDF) to be easily utilized. This is an advantage for both the propounding party and the responding party, since images of the documents can be linked to entries in the case analysis and support software.

9.52[2] Database Load File of Metadata Provides Relevant Information Concerning Document Image. When documents are converted into TIFF or PDF format (sometimes referred to as "near paper" format), vendors can also extract metadata about the documents and populate the data into a database. The database records are linked to the corresponding images. When the responding party produces the information, the TIFF or PDF files are produced in conjunction with a load file of the agreed-upon metadata for the images. The party receiving the TIFF or PDF files and the load file can import them into their own document management database system. The litigation software allows searching and sorting of the data, and easy display of the images.

9.52[3] Documents Produced in TIFF or PDF Format May Easily Be Redacted and Control-Labeled. Redaction of documents produced in TIFF or PDF format is easily accomplished during the review stage for privilege and responsiveness. However, both TIFF and PDF files that have been "redacted" by reviewers require further processing prior to production in order to truly eliminate the portions selected for redacting. Also, it is important to manually remove redacted text from text field of the database load file given to opposing counsel if the parties have agreed to exchange the document text in addition to the images.

➤ Cross Reference:

Redacting partially privileged documents, 9.44[2].

9.52[4] TIFF and PDF Formats Have Some Disadvantages. TIFF or PDF format productions may be difficult for attorneys without the appropriate software and technical staff to handle. This is especially true with productions consisting of TIFF files when single-page TIFF images are used—for a 50-page document, there would be 50 individual files. Having software that can recognize and group these 50 files is an imperative for all but the smallest productions.

 Cross Reference:

Disadvantages of TIFF and PDF formats for privilege review, see 9.38[2][*d*], [*e*].



177 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
VIII. PRODUCING DOCUMENTS TO THE DEMANDING PARTY

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.53

AUTHOR: Ernst Halperin

9.53 ESI Is Often Produced in Near-Native Format When Producing Large Compilations Derived From Searches of Large Databases.

Responsive data from a database is usually obtained by running queries against the database. The output of these queries is in structured format, usually in the form of some kind of tabular report that can be printed on paper. When the output is very large, the resulting data is often exported to an electronic data file. The output file is in "near-native" format because it is structured electronic data, but does not necessarily contain information from all of the fields in the original database. For instance, one protocol for this type of output file is known as "comma delimited," because the fields in the output report are separated by a comma. The producing party can give the demanding party information about the structure of the reported data (such as the field names), which the propounding party can then use to create its own database of results. If resulting data compilation is small enough, it can be imported into a spreadsheet.



178 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
VIII. PRODUCING DOCUMENTS TO THE DEMANDING PARTY

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.54

AUTHOR: Ernst Halperin

9.54 Production of ESI in Native Format Is Least Expensive But Can Be Problematic.

9.54[1] Native ESI Can Be the Most Useful Format and Least Expensive for Production. A production in native format can contain all the information that the native file held, including metadata such as Excel formulas, or last accessed/modified dates. It thus provides the most useful information about the ESI. It is also often an inexpensive way to produce ESI. The producing party does not have to spend the 8 cents to 15 cents per page cost of converting the files into TIFF format.

Example:

In a production of 3 gigabytes (equivalent to approximately 225,000 pages of information), which is not uncommon, the producing party would save between \$18,000 and \$34,000 in conversion costs.

9.54[2] Native Format Production Presents Difficulties in Handling and Review. Native file format presents difficulties in redaction, since redaction would require altering the actual file itself. One way to avoid this is to produce files that require redaction in another, non-native format such as TIFF, PDF, or paper.

Alternatively, if the native files are to be altered to remove privileged material, counsel should agree on a protocol for identifying when native format files have been altered to redact privileged data. The original, unredacted native files should be saved separately to allow resolution of any disputes if the receiving party believes the redactions have improperly removed unprivileged information.

Native format files also are easy to modify. This presents difficulties in being able to easily ensure that the data is not altered after being produced. Cooperation of counsel and well-documented procedures are required to allow effective use of native format evidence at depositions and trial. Most evidence at trial is in paper form, so the opposing lawyers need to stipulate to a procedure for authenticating native format ESI, including a method of being able to trace it back to the produced ESI. The Electronic Discovery Reference Model (ERDM) recommends "hashing" native files so that the hash values of the produced file can be compared with the hash value of other documents used in evidence at depositions or trial if there is any question of tampering. "Hashing" a file is the process of applying an algorithm to the file which calculates a calculated value that serves as a unique "fingerprint" of the file. Copies of a file will have a different hash values if they are different.

The ERDM recommends the following best practices for handling native format data [see ERDM (edrm.net), Evergreen, http://edrm.net/wiki2/index.php/Production_-_Form_of_Production#Special_Considerations_for_Native_Productions]:

- Hash the files. The most common hashing algorithm is known as an "MD5 hash."
- Organize the files into CD-sized volumes.
- Rename the files with the beginning Bates number as a suffix (for example, "Document.CDN00080.doc"). Renaming a file does not change the MD5 hash.
- Set the files to read-only. Doing this does not change the MD5 hash.
- Deliver an index with each CD volume containing the following information:
 - ☐ Volume.
 - ☐ Beginning Bates number.
 - ☐ MD5 hash value for the file.
 - ☐ Filename.
 - ☐ Modified filename. The recommended format is to include the original filename, the beginning Bates number, and the original extension, e.g., "Document.CDN00080.doc."
 - ☐ Provide the demanding party with the MD5 hash tool to verify the MD5 hash value on the index.



179 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
VIII. PRODUCING DOCUMENTS TO THE DEMANDING PARTY

*1-9 MB Practice Guide: CA E-Discovery and Evidence 9.55***AUTHOR:** Ernst Halperin**9.55 Timing the Production of ESI.**

9.55[1] Propounding Party May Not Specify Less Than 30 Days for Production of ESI. The party demanding production of ESI must "specify a reasonable time for the inspection, copying, testing, or sampling that is at least 30 days after service of the demand, unless the court for good cause shown has granted leave to specify an earlier date" [CCP § 2031.030(c)(2)].

9.55[2] Parties Should Agree to Production Schedule When Large Amounts of Data Are Likely to Require More Than 30 Days to Process and Produce. Many document demands are so broad that producing documents in response to them requires more than 30 days. The time necessary to complete discovery of ESI should be one of the topics addressed by counsel in initial meet and confer sessions [see *Cal Rules Ct, Rule 3.724(8)(C)*].

**Cross References:**

Meet and confer requirement and strategy, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference*, 5.14-5.21.

Response must specify time frame for document production, see *Ch. 8, Responding to Electronic Discovery Demands in California Court*, 8.11.

9.55[3] Rolling Production May Meet Both Parties' Objectives. The propounding party wants to get the information demanded as quickly as possible. The responding party needs adequate time to perform a diligent search, check for responsiveness, and perform privilege review. If a document production will take more than 30 days to process, a rolling production schedule can help meet both parties' legitimate objectives.

**Warning:**

When negotiating a rolling production, counsel for the producing party should be careful to negotiate realistic time deadlines for each tranche. Missing an interim production deadline is a surefire way to develop mistrust.

9.55[4] Choosing a Location for Production. The Electronic Discovery Act requires the demanding party to "specify a reasonable place for making the inspection, copying, testing, or sampling, and performing any relate activity" [CCP § 2031.030(c)(3)]. In practice, most document productions occur by delivering the end product to counsel for the propounding party. This is especially practical when the documents are produced as electronic files on a CD-ROM, DVD, or hard drive. Producing counsel may want to use a third-party delivery service and get a delivery confirmation with a signature in order to be able to prove when the propounding party received the documents.



180 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
VIII. PRODUCING DOCUMENTS TO THE DEMANDING PARTY

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.56

AUTHOR: Ernst Halperin

9.56 Counsel Should Document Each Production With Cover Letter Detailing What Was Produced.

Producing counsel will want to document what was produced and when. The best way to do this is to accompany each production with a cover letter listing what is included in the production, and maintaining well-labeled file copies of the CD-ROM or DVD disks included with the production.



Cross Reference:

Form, Sample Letter to Opposing Counsel Documenting Information Produced, see 9.60.



181 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
IX. FORMS

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.57

AUTHOR: Ernst Halperin

9.57 Sample Records Custodian Interview Checklist.

Sample Records Custodian Interview Checklist.

- ☐ Interview witness about his or her role in the dispute.
- ☐ Note source of any documents witness shows counsel during the interview about his or her role in the dispute. This will give a preliminary indication of where the custodian's relevant documents are likely to reside.
- ☐ Catalog electronic systems used by the witness.
 - ☐ E-mail:
 - ☐ How does the witness use the company's e-mail system? Does the witness regularly sort e-mails into subfolders, and if so, how are the subfolders organized in a manner that would enable counsel to make a reasoned, defensible decision to harvest e-mails from only certain subfolders?
 - ☐ How would the witness go about searching for electronic documents relevant to the case? Are there particular names or terms that would be useful in a search? Are there particular folders or other locations to search? Are there other witnesses to ask?
 - ☐ Does the witness back up e-mails onto the local hard drive or onto other media such as CD-ROM?

☐ Does the witness send relevant documents or e-mails to or from a personal e-mail account, perhaps when working from home?

☐ Does the witness know of any relevant information stored on an Internet site (e.g., Internet e-mail services such as Gmail or Yahoo! mail, blogs, document storage or backup sites, Twitter, etc.)?

☐ Word processing, spreadsheet and other office documents: What document management system, if any, is used?

☐ Does the witness always use the organization's document management system?

☐ If not, where does the witness store documents?

☐ Working out of the office and other media:

☐ Does the witness use a laptop?

☐ Does the witness use a smart phone or personal digital assistant for work?

☐ Does the witness carry work on flash disks or thumb drives?

☐ Does the witness back up any work information onto portable backup drives, CD-ROM, or older technologies such as Zip drives or floppy drives?

☐ Does the witness work from home?

☐ If so, on a company laptop or home computer?

☐ Are there any media used by the witness that can be ruled out as not reasonably likely to contain any responsive data?

☐ Has the witness used instant messaging, texting, or electronic voice mail systems? Are records of that archived anywhere? Does the witness continue to use these systems for data relevant to the case?

☐ Did the witness receive document preservation instructions? What did the witness do in response?

☐ Has any data from the relevant time periods been lost for any reason, e.g., a computer disk crash or migration between computer systems or software? If so, what were the circumstances? Can the data be retrieved from anywhere else?

NOTES:

Use and Content of Form:

See 9.13



Timing:

See 9.13[1]



182 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
IX. FORMS

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.58

AUTHOR: Ernst Halperin

9.58 San Mateo County Superior Court Model Stipulation and Protective Order Regarding Confidential Information (Single Level of Confidentiality).

San Mateo County Superior Court Model Stipulation and Protective Order Regarding Confidential Information (Single Level of Confidentiality).

STIPULATION AND PROTECTIVE ORDER REGARDING CONFIDENTIAL INFORMATION (Single Level of Confidentiality)

In order to protect confidential information obtained by the parties in connection with this case, the parties, by and through their respective undersigned counsel and subject to the approval of the Court, hereby agree as follows:

Part One: Use of Confidential Materials in Discovery

1. Any party or non-party may designate as "Confidential Information" (by stamping the relevant page or as otherwise set forth herein) any document or response to discovery which that party or non-party considers in good faith to contain information involving trade secrets, or confidential business or financial information, including personal financial information about any party to this lawsuit, putative class members or employee of any party to this lawsuit, information regarding any individual's banking relationship with any banking institution, information regarding the individual's financial transactions or financial accounts, and any information regarding any party not otherwise available to the public, subject to protection under *Rules 2.550, 2.551, 2.580, 2.585, 8.46, and 8.490 of the California Rules of Court* or under other provisions of California law. Where a document or response consists of more than one page, the first page and each page on which confidential information appears shall be so designated.
2. A party or non-party may designate information disclosed during a deposition or in response to written discovery as "Confidential" by so indicating in said responses or on the record at the deposition and demanding the preparation of a separate transcript of such material. In addition, a party or non-party may designate in writing, within thirty (30) days

after receipt of said responses or of the deposition transcript for which the designation is proposed, that specific pages of the transcript and/or specific responses be treated as "Confidential Information." Any other party may object to such proposal, in writing or on the record. Upon such objection, the parties shall follow the procedures described in Paragraph 8 below. After any designation made according to the procedure set forth in this paragraph, the designated documents or information shall be treated according to the designation until the matter is resolved according to the procedures described in Paragraph 8 below, and counsel for all parties shall be responsible for marking all previously unmarked copies of the designated material in their possession or control with the specified designation. A party that makes original documents or materials available for inspection need not designate them as Confidential Information until after the inspecting party has indicated which materials it would like copied and produced. During the inspection and before the designation and copying, all of the material made available for inspection shall be considered Confidential Information.

3. All Confidential Information produced or exchanged in the course of this case (not including information that is publicly available) shall be used by the party or parties to whom the information is produced solely for the purpose of this case. Confidential Information shall not be used for any commercial competitive, personal, or other purpose.

4. Except with the prior written consent of the other parties, or upon prior order of this Court obtained upon notice to opposing counsel, Confidential Information shall not be disclosed to any person other than:

(a) counsel for the respective parties to this litigation, including in-house counsel and co-counsel retained for this litigation;

(b) employees of such counsel;

(c) individual parties or officers or employees of a party, to the extent deemed necessary by counsel for the prosecution or defense of this litigation;

(d) consultants or expert witnesses retained for the prosecution or defense of this litigation, provided that each such person shall execute a copy of the Certification annexed to this Order (which shall be retained by counsel to the party so disclosing the Confidential Information and made available for inspection by opposing counsel during the pendency or after the termination of the action only upon good cause shown and upon order of the Court) before being shown or given any Confidential Information, and provided that if the party chooses a consultant or expert employed by the defendant or one of its competitors, the party shall notify the opposing party, or designating non-party, before disclosing any Confidential Information to that individual and shall give the opposing party an opportunity to move for a protective order preventing or limiting such disclosure;

(e) any authors or recipients of the Confidential Information;

(f) the Court, court personnel, and court reporters; and

(g) witnesses (other than persons described in Paragraph 4(e)). A witness shall sign the Certification before being shown a confidential document. Confidential Information may be disclosed to a witness who will not sign the Certification only in a deposition at which the party who designated the Confidential Information is represented or has been given notice that Confidential Information produced by the party may be used. At the request of any party, the portion of the deposition transcript involving the Confidential Information shall be designated "Confidential" pursuant to Paragraph 2 above. Witnesses shown Confidential Information shall not be allowed to retain copies.

5. Any persons receiving Confidential Information shall not reveal or discuss such information to or with any person who is not entitled to receive such information, except as set forth herein. If a party or any of its representatives, including counsel, inadvertently discloses any Confidential Information to persons who are not authorized to use or

possess such material, the party shall provide immediate written notice of the disclosure to the party whose material was inadvertently disclosed. If a party has actual knowledge that Confidential Information is being used or possessed by a person not authorized to use or possess that material, regardless of how the material was disclosed or obtained by such person, the party shall provide immediate written notice of the unauthorized use or possession to the party whose material is being used or possessed. No party shall have an affirmative obligation to inform itself regarding such possible use or possession.

6. In connection with discovery proceedings as to which a party submits Confidential Information, all documents and chamber copies containing Confidential Information which are submitted to the Court shall be filed with the Court in sealed envelopes or other appropriate sealed containers. On the outside of the envelopes, a copy of the first page of the document shall be attached. If Confidential Information is included in the first page attached to the outside of the envelopes, it may be deleted from the outside copy. The word "CONFIDENTIAL" shall be stamped on the envelope and a statement substantially in the following form shall also be printed on the envelope: "This envelope is sealed pursuant to Order of the Court, contains Confidential Information and is not to be opened or the contents revealed, except by Order of the Court or agreement by the parties." If another court or administrative agency subpoenas or orders production of Confidential Information, such party shall promptly notify counsel for the party who produced the material of the pendency of such subpoena or order and shall furnish counsel with a copy of said subpoena or order.

7. A party may designate as "Confidential Information" documents or discovery materials produced by a non-party by providing written notice to all parties of the relevant document numbers or other identification within thirty (30) days after receiving such documents or discovery materials. Any party or non-party may voluntarily disclose to others without restriction any information designated by that party or non-party as Confidential Information, although a document may lose its confidential status if it is made public. If a party produces materials designated Confidential Information in compliance with this Order, that production shall be deemed to have been made consistent with any confidentiality or privacy requirements mandated by local, state or federal laws.

8. If a party contends that any material is not entitled to confidential treatment, such party may at any time give written notice to the party or non-party who designated the material. The party or non-party who designated the material shall have twenty (20) days from such written notice to apply to the Court for an order designating the material as confidential. The party or non-party seeking the order has the burden of establishing that the document is entitled to protection.

9. Notwithstanding any challenge to the designation of material as Confidential Information, all documents shall be treated as such and shall be subject to the provisions hereof unless and until one of the following occurs:

- (a) The party or non-party who claims that the material is Confidential Information withdraws such designation in writing; or
- (b) The party or non-party who claims that the material is Confidential Information fails to apply to the Court for an order designating the material confidential within the time period specified above after receipt of a written challenge to such designation; or
- (c) The Court rules the material is not Confidential Information.

10. All provisions of this Order restricting the communication or use of Confidential Information shall continue to be binding after the conclusion of this action, unless otherwise agreed or ordered. Upon conclusion of the litigation, a party in the possession of Confidential Information, other than that which is contained in pleadings, correspondence, and deposition transcripts, shall either (a) return such documents no later than thirty (30) days after conclusion of this action to counsel for the party or non-party who provided such information, or (b) destroy such documents within the time period upon consent of the party who provided the information and certify in writing within thirty (30) days that the

documents have been destroyed.

11. Nothing herein shall be deemed to waive any applicable privilege or work product protection, or to affect the ability of a party to seek relief for an inadvertent disclosure of material protected by privilege or work product protection. Any witness or other person, firm, or entity from which discovery is sought may be informed of and may obtain the protection of this Order by written advice to the parties' respective counsel or by oral advice at the time of any deposition or similar proceeding.

Part Two: Use of Confidential Materials in Court

The following provisions govern the treatment of Confidential Information used at trial or submitted as a basis for adjudication of matters other than discovery motions or proceedings. These provisions are subject to *Rules 2.550, 2.551, 2.580, 2.585, 8.160, and 8.490 of the California Rules of Court* and must be construed in light of those Rules.

12. A party that files with the Court, or seeks to use at trial, materials designated as Confidential Information, and who seeks to have the record containing such information sealed, shall submit to the Court a motion or an application to seal, pursuant to *California Rule of Court 2.551*.

13. A party that files with the Court, or seeks to use at trial, materials designated as Confidential Information by anyone other than itself, and who does not seek to have the record containing such information sealed, shall comply with either of the following requirements:

(a) At least ten (10) business days prior to the filing or use of the Confidential Information, the submitting party shall give notice to all other parties, and to any non-party that designated the materials as Confidential Information pursuant to this Order, of the submitting party's intention to file or use the Confidential Information, including specific identification of the Confidential Information. Any affected party or non-party may then file a motion to seal, pursuant to *California Rule of Court 2.551(b)*; or

(b) At the time of filing or desiring to use the Confidential Information, the submitting party shall submit the materials pursuant to the lodging-under-seal provision of *California Rule of Court 2.551(d)*. Any affected party or non-party may then file a motion to seal, pursuant to the *California Rule of Court 2.551(b)*, within ten (10) business days after such lodging.

Documents lodged pursuant to *California Rule of Court 2.551(d)* shall bear a legend stating that such materials shall be unsealed upon expiration of ten (10) business days, absent the filing of a motion to seal pursuant to *Rule 2.551(b)* or Court order.

14. In connection with a request to have materials sealed pursuant to Paragraph 12 or Paragraph 13, the requesting party's declaration pursuant to *California Rule of Court 2.551(b)(1)* shall contain sufficient particularity with respect to the particular Confidential Information and the basis for sealing to enable the Court to make the findings required by *California Rule of Court 2.550(d)*.

IT IS SO STIPULATED.

Dated: _____ . By: _____ .

Dated: _____ . By: _____ .

ORDER

IT IS SO ORDERED.

Dated: _____ .

JUDGE OF THE SUPERIOR COURT

CERTIFICATION

I hereby certify my understanding that Confidential Information is being provided to me pursuant to the terms and restrictions of the Stipulation and Protective Order Regarding Confidential Information filed on _____, 200_____, in San Mateo County Superior Court Case No. _____ ("Order"). I have been given a copy of that Order and read it. I agree to be bound by the Order. I will not reveal the Confidential Information to anyone, except as allowed by the Order. I will maintain all such Confidential Information, including copies, notes, or other transcriptions made therefrom, in a secure manner to prevent unauthorized access to it. No later than thirty (30) days after the conclusion of this action, I will return the Confidential Information, including copies, notes, or other transcriptions made therefrom, to the counsel who provided me with the Confidential Information. I hereby consent to the jurisdiction of the San Mateo County Superior Court for the purpose of enforcing the Order.

I declare under penalty of perjury that the foregoing is true and correct and that this certificate is executed this _____ day of _____, 20_____, at _____.

By: _____

Address: _____

Phone: _____

NOTES:

Authority:

San Mateo County Superior Court Complex Litigation Program Complex Court Rules and Procedures.

NOTE: Obsolete reference to Cal. Rules of Court in official form has been updated by publisher's editorial staff.

Discussion of Use of Order:

See 9.18



Timing:

See 9.18



183 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
IX. FORMS

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.59

AUTHOR: Ernst Halperin

9.59 San Mateo County Superior Court Model Stipulation and Protective Order Regarding Confidential Information (Two Levels of Confidentiality).

San Mateo County Superior Court Model Stipulation and Protective Order Regarding Confidential Information (Two Levels of Confidentiality).

STIPULATION AND PROTECTIVE ORDER REGARDING CONFIDENTIAL INFORMATION (Two Levels of Confidentiality)

In order to protect confidential information obtained by the parties in connection with this case, the parties, by and through their respective undersigned counsel and subject to the approval of the Court, hereby agree as follows:

Part One: Use of Confidential Materials in Discovery

1. Any party or non-party may designate as "Confidential Information" (by stamping the relevant page or as otherwise set forth herein) any document or response to discovery which that party or non-party considers in good faith to contain information involving trade secrets, or confidential business or financial information, including personal financial information about any party to this lawsuit, putative class members or employee of any party to this lawsuit; information regarding any individual's banking relationship with any banking institution, including information regarding the individual's financial transactions or financial accounts, and any information regarding any party not otherwise available to the public, subject to protection under *Rules 2.550, 2.551, 2.580, 2.585, 8.46, and 8.490 of the California Rules of Court* or under other provisions of California law. Any party or non-party may designate as "Highly Confidential Information" (by stamping the relevant page or as otherwise set forth herein) any document or response to discovery which that party or non-party considers in good faith to contain information involving highly sensitive trade secrets or confidential business or financial information, the disclosure of which would result in the disclosure of trade secrets or other highly sensitive research, development, production, personnel, commercial, market, financial, or business information, subject to protection under *Rules 2.550, 2.551, 2.580, 2.585, 8.160, and 8.490 of the California*

Rules of Court or under other provisions of California law. Where a document or response consists of more than one page, the first page and each page on which confidential information appears shall be so designated.

2. A party or non-party may designate information disclosed during a deposition or in response to written discovery as "Confidential" or "Highly Confidential" by so indicating in said responses or on the record at the deposition and requesting the preparation of a separate transcript of such material. In addition, a party or non-party may designate in writing, within thirty (30) days after receipt of said responses or of the deposition transcript for which the designation is proposed, that specific pages of the transcript and/or specific responses be treated as "Confidential Information" or "Highly Confidential." Any other party may object to such proposal, in writing or on the record. Upon such objection, the parties shall follow the procedures described in Paragraph 9 below. After any designation made according to the procedure set forth in this paragraph, the designated documents or information shall be treated according to the designation until the matter is resolved according to the procedures described in Paragraph 9 below, and counsel for all parties shall be responsible for marking all previously unmarked copies of the designated material in their possession or control with the specified designation. A party that makes original documents or materials available for inspection need not designate them as Confidential or Highly Confidential Information until after the inspecting party has indicated which materials it would like copied and produced. During the inspection and before the designation and copying, all of the material made available for inspection shall be considered Confidential or Highly Confidential Information.

3. All Confidential or Highly Confidential Information produced or exchanged in the course of this case (not including information that is publicly available) shall be used by the party or parties to whom the information is produced solely for the purpose of this case. Confidential or Highly Confidential Information shall not be used for any commercial competitive, personal, or other purpose.

4. Except with the prior written consent of the other parties, or upon prior order of this Court obtained upon notice to opposing counsel, Confidential Information shall not be disclosed to any person other than:

(a) counsel for the respective parties to this litigation, including in-house counsel and co-counsel retained for this litigation;

(b) employees of such counsel;

(c) individual parties or officers or employees of a party, to the extent deemed necessary by counsel for the prosecution or defense of this litigation;

(d) consultants or expert witnesses retained for the prosecution or defense of this litigation, provided that each such person shall execute a copy of the

Certification annexed to this Order (which shall be retained by counsel to the party so disclosing the Confidential Information and made available for inspection by opposing counsel during the pendency or after the termination of the action only upon good cause shown and upon order of the Court) before being shown or given any Confidential Information, and provided that if the party chooses a consultant or expert employed by the defendant or one of its competitors, the party shall notify the opposing party, or designating non-party, before disclosing any Confidential Information to that individual and shall give the opposing party an opportunity to move for a protective order preventing or limiting such disclosure;

(e) any authors or recipients of the Confidential Information;

(f) the Court, court personnel, and court reporters; and

(g) witnesses (other than persons described in Paragraph 4(e)). A witness shall sign the Certification before being shown

a confidential document. Confidential Information may be disclosed to a witness who will not sign the Certification only in a deposition at which the party who designated the Confidential Information is represented or has been given notice that Confidential Information produced by the party may be used. At the request of any party, the portion of the deposition transcript involving the Confidential Information shall be designated "Confidential" pursuant to Paragraph 2 above. Witnesses shown Confidential Information shall not be allowed to retain copies.

5. Except with the prior written consent of the other parties, or upon prior order of this Court obtained after notice to opposing counsel, Highly Confidential Information shall be treated in the same manner as "Confidential Information" pursuant to Paragraph 4 above, except that it shall not be disclosed to individual parties or directors, officers or employees of a party.

6. Any persons receiving Confidential or Highly Confidential Information shall not reveal or discuss such information to or with any person who is not entitled to receive such information, except as set forth herein. If a party or any of its representatives, including counsel, inadvertently discloses any Confidential or Highly Confidential Information to persons who are not authorized to use or possess such material, the party shall provide immediate written notice of the disclosure to the party whose material was inadvertently disclosed. If a party has actual knowledge that Confidential or Highly Confidential Information is being used or possessed by a person not authorized to use or possess that material, regardless of how the material was disclosed or obtained by such person, the party shall provide immediate written notice of the unauthorized use or possession to the party whose material is being used or possessed. No party shall have an affirmative obligation to inform itself regarding such possible use or possession.

7. In connection with discovery proceedings as to which a party submits Confidential or Highly Confidential Information, all documents and chamber copies containing Confidential or Highly Confidential Information which are submitted to the Court shall be filed with the Court in sealed envelopes or other appropriate sealed containers. On the outside of the envelopes, a copy of the first page of the document shall be attached. If Confidential or Highly Confidential Information is included in the first page attached to the outside of the envelopes, it may be deleted from the outside copy. The word "CONFIDENTIAL" shall be stamped on the envelope and a statement substantially in the following form shall also be printed on the envelope:

"This envelope is sealed pursuant to Order of the Court, contains Confidential Information and is not to be opened or the contents revealed, except by Order of the Court or agreement by the parties."

If another court or administrative agency subpoenas or orders production of Confidential or Highly Confidential Information, such party shall promptly notify counsel for the party who produced the material of the pendency of such subpoena or order and shall furnish counsel with a copy of said subpoena or order.

8. A party may designate as "Confidential Information" or "Highly Confidential Information" documents or discovery materials produced by a non-party by providing written notice to all parties of the relevant document numbers or other identification within thirty (30) days after receiving such documents or discovery materials. Any party or non-party may voluntarily disclose to others without restriction any information designated by that party or non-party as Confidential or Highly Confidential Information, although a document may lose its confidential status if it is made public. If a party produces materials designated Confidential or Highly Confidential Information in compliance with this Order, that production shall be deemed to have been made consistent with any confidentiality or privacy requirements mandated by local, state or federal laws.

9. If a party contends that any material is not entitled to confidential treatment, such party may at any time give written notice to the party or non-party who designated the material. The party or non-party who designated the material shall have twenty (20) days from the receipt of such written notice to apply to the Court for an order designating the material as confidential. The party or non-party seeking the order has the burden of establishing that the document is entitled to protection.

10. Notwithstanding any challenge to the designation of material as Confidential or Highly Confidential Information, all documents shall be treated as such and shall be subject to the provisions hereof unless and until one of the following occurs:

- (a) The party or non-party who claims that the material is Confidential or Highly Confidential Information withdraws such designation in writing; or
- (b) The party or non-party who claims that the material is Confidential or Highly Confidential Information fails to apply to the Court for an order designating the material confidential within the time period specified above after receipt of a written challenge to such designation; or
- (c) The Court rules the material is not Confidential or Highly Confidential Information.

11. All provisions of this Order restricting the communication or use of Confidential or Highly Confidential Information shall continue to be binding after the conclusion of this action, unless otherwise agreed or ordered. Upon conclusion of the litigation, a party in the possession of Confidential or Highly Confidential Information, other than that which is contained in pleadings, correspondence, and deposition transcripts, shall either (a) return such documents no later than thirty (30) days after conclusion of this action to counsel for the party or non-party who provided such information, or (b) destroy such documents within the time period upon consent of the party who provided the information and certify in writing within thirty (30) days that the documents have been destroyed.

12. Nothing herein shall be deemed to waive any applicable privilege or work product protection, or to affect the ability of a party to seek relief for an inadvertent disclosure of material protected by privilege or work product protection. Any witness or other person, firm or entity from which discovery is sought may be informed of and may obtain the protection of this Order by written advice to the parties' respective counsel or by oral advice at the time of any deposition or similar proceeding.

Part Two: Use of Confidential Materials in Court

The following provisions govern the treatment of Confidential or Highly Confidential Information used at trial or submitted as a basis for adjudication of matters other than discovery motions or proceedings. These provisions are subject to *Rules 2.550, 2.551, 2.580, 2.585, 8.160, and 8.490 of the California Rules of Court* and must be construed in light of those Rules.

13. A party that files with the Court, or seeks to use at trial, materials designated as Confidential or Highly Confidential Information, and who seeks to have the record containing such information sealed, shall submit to the Court a motion or an application to seal, pursuant to *California Rule of Court 2.551*.

14. A party that files with the Court, or seeks to use at trial, materials designated as Confidential or Highly Confidential Information by anyone other than itself, and who does not seek to have the record containing such information sealed, shall comply with either of the following requirements:

- (a) At least ten (10) business days prior to the filing or use of the Confidential or Highly Confidential Information, the submitting party shall give notice to all other parties, and to any non-party that designated the materials as Confidential or Highly Confidential Information pursuant to this Order, of the submitting party's intention to file or use the Confidential or Highly Confidential Information, including specific identification of the Confidential or Highly Confidential Information. Any affected party or non-party may then file a motion to seal, pursuant to *California Rule of Court 2.551(b)*; or

(b) At the time of filing or desiring to use the Confidential or Highly Confidential Information, the submitting party shall submit the materials pursuant to the lodging-under-seal provision of *California Rule of Court 2.551(d)*. Any affected party or non-party may then file a motion to seal, pursuant to the *California Rule of Court 2.551(b)*, within ten (10) business days after such lodging. Documents lodged pursuant to *California Rule of Court 2.551(d)* shall bear a legend stating that such materials shall be unsealed upon expiration of ten (10) business days, absent the filing of a motion to seal pursuant to *Rule 2.551(b)* or Court order.

15. In connection with a request to have materials sealed pursuant to Paragraph 12 or Paragraph 13, the requesting party's declaration pursuant to *California Rule of Court 2.551(b)(1)* shall contain sufficient particularity with respect to the particular Confidential or Highly Confidential Information and the basis for sealing to enable the Court to make the findings required by *California Rule of Court 2.550(d)*.

IT IS SO STIPULATED.

Dated: _____ . By: _____ .

Dated: _____ . By: _____ .

ORDER

IT IS SO ORDERED.

Dated: _____ .

JUDGE OF THE SUPERIOR COURT

CERTIFICATION

I hereby certify my understanding that Confidential or Highly Confidential Information is being provided to me pursuant to the terms and restrictions of the Stipulation and Protective Order Regarding Confidential Information filed on _____, 200____, in San Mateo County Superior Court Case No. _____ ("Order"). I have been given a copy of that Order and read it. I agree to be bound by the Order. I will not reveal the Confidential or Highly Confidential Information to anyone, except as allowed by the Order. I will maintain all such Confidential or Highly Confidential Information, including copies, notes, or other transcriptions made therefrom, in a secure manner to prevent unauthorized access to it. No later than thirty (30) days after the conclusion of this action, I will return the Confidential or Highly Confidential Information, including copies, notes, or other transcriptions made therefrom, to the counsel who provided me with the Confidential or Highly Confidential Information. I hereby consent to the jurisdiction of the San Mateo County Superior Court for the purpose of enforcing the Order.

I declare under penalty of perjury that the foregoing is true and correct and that this certificate is executed this _____ day of _____, 20____, at _____.

By: _____

Address: _____

Phone: _____

NOTES:

Authority:

San Mateo County Superior Court Complex Litigation Program Complex Court Rules and Procedures.

NOTE: Obsolete reference to Cal. Rules of Court in official form has been updated by publisher's editorial staff.

Discussion of Use of Order:

See 9.18



Timing:

See 9.18



184 of 184 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 9 Gathering and Producing Electronically Stored Information
IX. FORMS

1-9 MB Practice Guide: CA E-Discovery and Evidence 9.60

AUTHOR: Ernst Halperin

9.60 Sample Letter to Opposing Counsel Documenting Information Produced.

Sample Letter to Opposing Counsel Documenting Information Produced.

[date]

VIA _____ [name of delivery service or carrier]

Mr. Tom Doe
100 North Main St., Suite 200
Farallon City, California 90000
Phone: 555-555-5555

Re: Smith v. Mary Jones Enterprises, Inc.

Dear Mr. Doe,

Enclosed with this letter please find documents produced in response to Defendant's fifth Demand for Production of Documents. Unless otherwise noted, the documents are provided in TIFF format with load files containing the agreed-upon metadata, on the following CD-ROM disks:

Disk 1: Documents from the following witnesses:

Custodian:	Beginning Bates Range	End Bates Range
John Smith	Plaintiff0000001	Plaintiff0000459
Jane Doe	Plaintiff0000460	Plaintiff0012336

Disk 2: Output from stipulated queries to the customer database, responsive to Demands for Production Nos. 37 through 42. The files are in comma-delimited format. All of the output is designated "Highly Confidential" pursuant to the

stipulated protective order in place in this litigation.

Sincerely,

Jane Lee
California Bar Number 123456
50 South Main St., Suite 100
Farallon City, California 90000
Phone: 555-999-9999
Attorney for Defendant, Mary Jones Enterprises, Inc.

NOTES:

Discussion of Use and Content of Notice:

See 9.56



Timing:

See 9.56



1 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 10 Opposing Demands for Production of Electronic Evidence in California Court

1-10 MB Practice Guide: CA E-Discovery and Evidence 10.syn

§ 10.syn Synopsis to Chapter 10: Opposing Demands for Production of Electronic Evidence in California Court

10.01 Scope.

10.02 Objective and Strategy.

10.03 CHECKLIST: Determining Whether Grounds for Objection Exist.

10.04 Options and Strategies.

10.05 Responding Party May Object to Timing or Format of Demand for Production.

10.05[1] Plaintiff's Initial Demand Must Not Be Served Too Soon.

10.05[2] Demand Generally Must Not Be Served After Close of Discovery.

10.05[3] Demand Must Designate Information Sought With Reasonable Particularity.

10.06 Responding Party May Object on Relevance Grounds.

10.07 Responding Party May Object on Grounds of Undue Burden.

10.07[1] Responding Party May Object to Producing Information in Form Specified in Demand.

10.07[2] Responding Party May Object to Demand for Information That Is Not Reasonably Accessible.

10.07[3] Responding Party May Object to Demand That Is Cumulative or Burdensome Under Circumstances.

10.08 Responding Party May Object on Grounds of Confidentiality or Privilege.

10.08[1] Privileged Information Is Outside Scope of Discovery.

10.08[2] Privilege May Be Waived or Forfeited.

10.08[3] Responding Party Need Not Produce Material Protected by Attorney-Client Privilege.

10.08[4] Responding Party Need Not Produce Material Protected As Attorney Work Product.

10.08[5] Responding Party Need Not Produce Trade Secrets.

10.08[6] Public Entity Need Not Produce Official Information.

10.08[7] Responding Party Need Not Produce Information Protected by Other Privileges.

10.09 CHECKLIST: Asserting Objections to Production Demands.

10.10 Options and Strategies.

10.11 Responding Party May Assert Objections in Response to Demand.

10.11[1] Response Should Comply With Formal Requirements.

10.11[2] Privilege Log Need Not Be Prepared Unless Demanding Party Moves to Compel.

10.11[3] Demanding Party May Move for Further Response.

10.12 Responding Party May Seek Protective Order.

10.12[1] Objection May Be Asserted in Motion for Protective Order.

10.12[2] Court May Issue Protective Order on Ground That Information Is Inaccessible or on Other Traditional Grounds.

10.12[3] Court Has Broad Power to Tailor Protective Order.

10.12[4] Even If Court Orders Discovery, It May Impose Conditions and Allocate Costs.

10.12[5] Even If Protective Order Is Denied, Court Must Limit Frequency or Extent of Cumulative or Burdensome Discovery.

10.13 Responding Party May Move for Relief From Forfeiture of Objections After Failure to Serve Timely Response.

10.14 Responding Party May Seek Return of Inadvertently Disclosed Privileged Material.

10.15 Notice of Motion and Motion for Relief From Waiver of Objections to Demand for Production of Electronically Stored Information.

10.16 Declaration of Counsel in Support of Motion for Relief From Waiver of Objections to Demand for Production of Electronically Stored Information.

10.17 Order Granting Relief From Waiver of Objections to Demand for Production of Electronically Stored Information.



2 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 10 Opposing Demands for Production of Electronic Evidence in California Court
I. STRATEGY

1-10 MB Practice Guide: CA E-Discovery and Evidence 10.01

10.01 Scope.

This chapter covers the considerations and procedures involved in opposing a demand for production of electronically stored information, including:

- Determining whether grounds for objection exist [*see 10.03-10.08*].
- Asserting objections [*see 10.09-10.14*; Forms: *see 10.15-10.17*].

Objections to a production demand are typically asserted in a response to the demand. For discussion of the procedures for preparing and serving a response to a demand, including a comprehensive response form illustrating typical objections, see Ch. 8, Responding to Electronic Discovery Demands in California.

This chapter does not cover the procedures for gathering and producing electronically stored information. For discussion of those procedures, see Ch. 9, Gathering and Producing Electronically Stored Information.

This chapter does not cover the procedures for seeking or opposing a motion for a protective order. For discussion of those procedures, see Ch. 11, Seeking or Opposing Protective Order.

This chapter does not cover the procedures for making or opposing a motion to compel a response or to compel production. For discussion of those procedures, see Ch. 12, Obtaining or Opposing Motion to Compel.

This chapter does not cover the procedures for seeking or opposing sanctions for noncompliance with a demand to produce electronically stored information. For discussion of those procedures, see Ch. 13, Seeking or Opposing Sanctions for Noncompliance.

Core Statutes:

CCP §§ 2031.210, 2031.240, 2031.285, 2031.300



3 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 10 Opposing Demands for Production of Electronic Evidence in California Court
I. STRATEGY

1-10 MB Practice Guide: CA E-Discovery and Evidence 10.02

10.02 Objective and Strategy.

The decision to oppose all or part of a demand for production of electronically stored information should be considered part of counsel's overall strategy for e-discovery. When a demand for production is received, therefore, it is likely that the responding party will agree to provide some requested items and find other items objectionable. Any objections may be asserted in a response to the demand or in a motion for a protective order. Therefore, a comprehensive response strategy will include consideration of issues involved in the production of evidence and in seeking protective orders.



Cross References:

Discussion of determining whether grounds for objection exist, see *10.03-10.08*.

Discussion of asserting objections, see *10.09-10.14*.

Discussion of strategy and procedures for responding to production demand, see Ch. 8, Responding to Electronic Discovery Demands in California.

Discussion of gathering and producing electronically stored information, see Ch. 9, Gathering and Producing Electronically Stored Evidence.

Discussion of protective orders, see Ch. 12, Seeking or Opposing Protective Order.



4 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 10 Opposing Demands for Production of Electronic Evidence in California Court

II. DETERMINING WHETHER GROUNDS FOR OBJECTION EXIST

1-10 MB Practice Guide: CA E-Discovery and Evidence 10.03

10.03 CHECKLIST: Determining Whether Grounds for Objection Exist.

☐ Review demand for discovery of electronically stored information promptly after receiving it, to determine whether timing or format of demand is objectionable.

☐ If demand is plaintiff's initial demand, consider whether demand was served before expiration of 10 days (five days in unlawful-detainer action) after service of summons on, or appearance by, responding party, unless court has granted plaintiff leave to serve demand earlier.

Authority:

CCP § 2031.020(b)-(d)

Discussion:

See 10.05[1]

☐ Consider whether demand was served in time to allow for production of demanded information by discovery cutoff.

Authority:

CCP §§ 2024.020, 2031.030(c)(2)

Discussion:

See 10.05[2]

☐ Consider whether demand fails to designate information sought either by specifically describing each individual item or by reasonably particularizing each category of item.

Authority:

CCP § 2031.030(c)(1)

Discussion:

See 10.05[3]

- ☐ Determine whether any specific demand is objectionable on relevance grounds.

Authority:

CCP §§ 2017.010, 2031.010(a)

Discussion:

See 10.06

- ☐ Determine whether any particular demand is objectionable on grounds of undue burden.

- ☐ Consider whether demand seeks production of information in unreasonable format.

Authority:

CCP § 2031.280(c), (d)

Discussion:

See 10.07[1]

- ☐ Consider whether demand seeks production of information from source that is not reasonably accessible.

Authority:

CCP § 2031.210(d)

Discussion:

See 10.07[2]

- ☐ Consider whether any of following apply:

Authority:

CCP §§ 2019.030(a), 2031.060(f)

Discussion:

See 10.07[3]

☐ It is possible to obtain demanded information from some other source that is more convenient, less burdensome, or less expensive.

☐ Discovery sought is unreasonably cumulative or duplicative.

☐ Demanding party has had ample opportunity for discovery in action to obtain information sought.

- ☐ Likely burden or expense outweighs likely benefit, considering amount in controversy, resources of parties, importance of issues, and importance of demanded information in resolving issues.
- ☐ Determine whether any information demanded is subject to claim of privilege or confidentiality.
- ☐ Consider following privileges and protections:

☐ Attorney-client privilege.

Authority:

Evid Code §§ 954, 955

Discussion:

See 10.08[3]

- ☐ Attorney work product protection.

Authority:

CCP § 2018.030

Discussion:

See 10.08[4]

- ☐ Privilege for trade secrets.

Authority:

Evid Code § 1060; see CC § 3426.1(d)

Discussion:

See 10.08[5]

- ☐ Privilege for official information.

Authority:

Evid Code §§ 1040, 1041

Discussion:

See 10.08[6]

- ☐ Other constitutional and statutory privileges.

Discussion:

See 10.08[7]

- ☐ Verify that any applicable privilege or protection has not been waived or forfeited.

Authority:

CCP § 2031.300(a); Evid Code § 912; Venture Law Group v. Superior Court (2004) 118 CA4th 96, 105, 12 CR3d 656 ; McKesson HBOC, Inc. v. Superior Court (2004) 115 CA4th 1229, 1239, 9 CR3d 812

Discussion:

See 10.08[2]



5 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 10 Opposing Demands for Production of Electronic Evidence in California Court

II. DETERMINING WHETHER GROUNDS FOR OBJECTION EXIST

1-10 MB Practice Guide: CA E-Discovery and Evidence 10.04

10.04 Options and Strategies.

On receiving a demand for the production of electronically stored information, counsel for the responding party should promptly review the demand to assess whether any materials within the scope of the demand are subject to objection based on relevance, privilege, or other permissible legal bases.



Timing:

As soon as a production demand is received, counsel should determine when the response will be due, and then make sure that any relevant objections are determined in time to assert them by the response date. A failure to timely object or respond to a request for production ordinarily will result in the forfeiture of any objections, including those based on privilege or work-product protection [CCP § 2031.300(a)]. Generally, a response must be served within 30 days after service of the demand (five days after service of the demand, in an unlawful detainer action), unless the court has shortened or extended the time to respond or the parties have agreed in writing to an extended date for serving a response [CCP §§ 2031.260, 2031.270].



Cross Reference:

Discussion of motion for relief from forfeiture of objections, see 10.13.



6 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 10 Opposing Demands for Production of Electronic Evidence in California Court

II. DETERMINING WHETHER GROUNDS FOR OBJECTION EXIST

1-10 MB Practice Guide: CA E-Discovery and Evidence 10.05

10.05 Responding Party May Object to Timing or Format of Demand for Production.

10.05[1] Plaintiff's Initial Demand Must Not Be Served Too Soon. The plaintiff may not make a demand for production of electronically stored information until 10 days after service of the summons on, or appearance by, the party to whom the demand is directed [CCP § 2031.020(b)]. A premature demand is therefore objectionable.

Exception:

In an unlawful-detainer action, the plaintiff may serve a demand for production at any time that is five days after service of the summons on, or appearance by, the party to whom the demand is directed [CCP § 2031.020(c)].

Distinguish:

A defendant may make a demand for production of electronically stored information at any time [CCP § 2031.020(a)].



Cross Reference:

Discussion of procedure for demanding production of electronically stored information, see Ch. 6, Demanding Production of Electronically Stored Information in California Court.

10.05[2] Demand Generally Must Not Be Served After Close of Discovery. The parties ordinarily must complete all discovery by the 30th day before the initial date set for trial [CCP § 2024.020(a)]. A continuance or postponement of the trial date does not operate to reopen discovery proceedings [CCP § 2024.020(b)]. Therefore, because a demand generally must specify a reasonable time for production that is at least 30 days after service of the demand [CCP § 2031.030(c)(2)], a demand served fewer than 30 days before the discovery cutoff date is ordinarily objectionable.

Exceptions:

The usual discovery cutoff date is subject to two major exceptions.

- On motion by a party, the court may grant leave to complete discovery fewer than 30 days before the initial date set for trial, or to reopen discovery after a new trial date has been set [CCP § 2024.050(a)]. In

ruling on such a motion, the court considers (1) the necessity and the reasons for the discovery; (2) the diligence or lack of diligence of the party seeking the discovery, and the reasons that the discovery was not completed earlier; (3) any likelihood that permitting the discovery will prevent the case from going to trial on the date set, interfere with the trial calendar, or result in prejudice to any other party; and (4) the length of time that has elapsed between any date previously set, and the date currently set, for trial [CCP § 2024.050(b)].

■ The setting of a new trial date after a mistrial, an order granting a new trial, or a remand after appellate reversal of judgment automatically reopens discovery [*Fairmont Ins. Co. v. Superior Court* (2000) 22 C4th 245, 250-253, 92 CR2d 70, 991 P2d 156] .

Distinguish:

The Civil Discovery Act authorizes a party to propound supplemental demands for production of electronically stored information, including one supplemental demand after the initial setting of a trial date [CCP § 2031.050]. That authorization, however, does not create an exception to the generally applicable discovery cutoff. The Act expressly subjects supplemental production demands to the discovery cutoff [CCP § 2031.050(b); see CCP § 2024.050].



Cross Reference:

Discussion of discovery cutoff dates and methods for obtaining extensions under California law, see *Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 1, 1.17*.

10.05[3] Demand Must Designate Information Sought With Reasonable Particularity. A demand for production of electronically stored information must designate the information sought either by specifically describing each individual item or by reasonably particularizing each category of item [CCP § 2031.030(c)(1)]. Therefore, a demand that does not designate the information sought with sufficient particularity is objectionable [see *Calcor Space Facility, Inc. v. Superior Court* (1997) 53 CA4th 216, 223, 61 CR2d 567 (party's voluminous request for production accompanied by three pages of "definitions" and another three pages of "instructions" essentially amounted to impermissible blanket request for all documents that in any way related to subject matter of litigation)].



7 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 10 Opposing Demands for Production of Electronic Evidence in California Court
II. DETERMINING WHETHER GROUNDS FOR OBJECTION EXIST

1-10 MB Practice Guide: CA E-Discovery and Evidence 10.06

10.06 Responding Party May Object on Relevance Grounds.

Electronically stored information is within the scope of discovery if (1) it is not privileged, (2) it is relevant to the subject matter of the pending action or to the determination of any motion in the action, and (3) it is admissible in evidence or appears reasonably calculated to lead to the discovery of admissible evidence [*CCP* § 2017.010; *see CCP* § 2031.010(a)].

The information demanded may relate to the claim or defense of the demanding party or of any other party to the action. Additionally, a demanding party may obtain the identity and location of people with knowledge of any discoverable electronic information, including its existence, description, nature, custody, condition, and location [*CCP* § 2017.010]. Therefore, a production demand that seeks information that is outside the scope of discovery is objectionable [*see Nelson v. Superior Court* (1986) 184 CA3d 444, 450, 229 CR 94 (denying plaintiff's motion to compel California Highway Patrol to produce traffic accident reports because demanding party did not show that underlying request for production was reasonably calculated to lead to discovery of admissible evidence)].

Distinguish:

The scope of discovery under California Civil Discovery Act, which authorizes discovery of material that is relevant to the "subject matter involved in the pending action," is broader than the available scope of discovery under the Federal Rules of Civil Procedure [*CCP* § 2017.010]. The Federal Rules were amended in 2000 to limit the general scope of discovery to matters relevant to "any party's claim or defense"; discovery of material relevant to the "subject matter involved in the action" is available only if ordered by the court for good cause [*Fed R Civ P* 26(b)(2)].



Cross Reference:

Discussion of scope of discovery, *see* Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 2, Scope of Discovery.



8 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 10 Opposing Demands for Production of Electronic Evidence in California Court
II. DETERMINING WHETHER GROUNDS FOR OBJECTION EXIST

1-10 MB Practice Guide: CA E-Discovery and Evidence 10.07

10.07 Responding Party May Object on Grounds of Undue Burden.

10.07[1] Responding Party May Object to Producing Information in Form Specified in Demand. The responding party may object to producing information in the form specified in the demand [CCP § 2031.280(c)]. In such a case, the responding party's remedy is not to withhold production, but rather to state in the response the form in which it will produce the demanded information [CCP § 2031.280(c)]. Production must be either in the form in which the information is ordinarily maintained or in a form that is reasonably usable, unless the parties agree to a different format or the court issues an order specifying a certain format [CCP § 2031.280(d)].



Strategic Point:

If it is necessary to translate any data compilation into a reasonably usable form, the responding party must perform the translation at the expense of the demanding party [CCP § 2031.280(e); see *Toshiba Am. Elec. Components, Inc. v. Superior Court* (2004) 124 CA4th 762, 769-772, 21 CR3d 532 (cost-shifting under substantially identical predecessor of CCP § 2031.280(e) is mandatory); see also CCP § 1985.8(g) (similar requirement when nonparty is subpoenaed to produce electronically stored information); cf. CCP § 2031.060(e) (court may allocate costs of producing information that is not reasonably accessible)]. Therefore, if the responding party objects to producing information in the form specified by the demand, and translation is necessary, counsel should include in the response to the demand a statement of the expected cost of translation. If necessary, counsel should be prepared to make a motion for an award of translation costs.



Cross References:

Discussion of objection to production of information that is not reasonably accessible, see 10.07[2].

Discussion of Motion for Protective Order, see Ch. 11, Seeking or Opposing Protective Order.

Discussion of court's power to allocate cost of translation or production, see 10.12[4].

Discussion of procedures for responding to demand for production, see Ch. 8, Responding to Electronic

Discovery Demands in California Court.

10.07[2] Responding Party May Object to Demand for Information That Is Not Reasonably Accessible. The responding party may object to the discovery of electronically stored evidence on the grounds that it is from a source that is not reasonably accessible because of undue burden or expense [*CCP* § 2031.210(d)].

In determining whether a given source of electronically stored information is inaccessible because of undue burden and expense [*see CCP* § 2031.210(d)], the relevant burden and expense are those involved in putting the demanded information into a usable form. Thus, information generally is considered accessible if it is stored in a readily usable format and does not need to be restored or otherwise manipulated to be usable. Inaccessible data, on the other hand, is not readily usable [*see Zubulake v. UBS Warburg LLC (SDNY 2003) 217 FRD 309, 318-320* ("Whether electronic data is accessible or inaccessible turns largely on the media on which it is stored"); *see, e.g., Hill v. Eddie Bauer (CD Cal 2007) 242 FRD 556, 564-565* (plaintiff's request for production of electronic information was unduly burdensome, in part, because it would require 600 person-hours to identify and gather requested information)].

Examples:

Examples of accessible sources include computer hard drives, optical disks, and offline storage or archives that use magnetic tapes or optical disks. For such sources, the time it takes to actually access the data can range from milliseconds to days, but the data is considered accessible because it does not need to be restored or otherwise manipulated to be usable. In contrast, backup tapes or erased, fragmented, or damaged data are not considered accessible: backup tapes must be restored, fragmented data must be de-fragmented, and erased data must be reconstructed before it can be used [*see Zubulake v. UBS Warburg LLC (SDNY 2003) 217 FRD 309, 318-320*].

Distinguish--Inability to Comply:

Information that is not reasonably accessible because of undue burden or expense is different from information that the responding party is unable to produce under any circumstances. Rather than objecting to a demand for such information, the responding party may make a representation of inability to comply with the demand. A representation of inability to comply must (1) affirm that a diligent search and a reasonable inquiry have been made in an effort to comply with the demand; and (2) specify whether the information has never existed, has been destroyed, has been lost, misplaced, or stolen, or has never been, or is no longer, in the possession, custody, or control of the responding party. The representation of inability to comply must also set forth the name and address of any natural person or organization known or believed by the responding party to have possession, custody, or control of that item or category of item [*CCP* § 2031.230].

 Cross References:

Discussion of assertion of inaccessibility objection in response to demand, *see 10.07[2]*.

Discussion of representation of inability to comply, *see Ch. 8, Responding to Electronic Discovery Demands in California Court, 8.19*.

Discussion of court's power to allocate cost of production of information from inaccessible source, *see 10.12[4]*.

Discussion of protective orders generally, *see Ch. 11, Seeking or Opposing Protective Order*.

10.07[3] Responding Party May Object to Demand That Is Cumulative or Burdensome Under Circumstances. The court must issue a limiting order restricting the frequency or extent of discovery of electronically stored information, even from a source that is reasonably accessible, if it determines that any of the following conditions

exists [*CCP* § 2031.060(f); *see CCP* § 2019.030(a)]:

- It is possible to obtain the demanded information from some other source that is more convenient, less burdensome, or less expensive.
- The discovery sought is unreasonably cumulative or duplicative.
- The demanding party has had ample opportunity for discovery in the action to obtain the information sought.
- The likely burden or expense outweighs the likely benefit, considering the amount in controversy, resources of the parties, importance of the issues, and importance of the demanded information in resolving the issues.

Example--Unreasonably Cumulative or Duplicative Discovery:

Information often exists in multiple locations and formats. For example, hard-copy paper files may duplicate e-mail versions of the same documents, and a party may try to object to the production of both formats as duplicative [*see Williams v. Owens-Illinois, Inc.* (9th Cir 1982) 665 F2d 918, 932-933 (trial court's refusal to require defendants to produce their computer tapes was not abuse of discretion, since defendants had produced hard copy containing all information computer tapes contained)]. However, courts will often order production in more than one format, recognizing that the electronic form may be more convenient to search and that it is often difficult to confirm that there is complete overlap between two sources of documents [*see TBG Ins. Servs. Corp. v. Superior Court* (2002) 96 CA4th 443, 448-449, 117 CR2d 155 ("[A party] is entitled to discover any nonprivileged information, cumulative or not, that may reasonably assist it in evaluating its defense, preparing for trial, or facilitating a settlement")].

Example--Information Obtainable From Other Source:

In one case, a demand for production of documents that would have required plaintiff (the State of California) to search for documents from nonparty state agencies was held to be unduly burdensome [*see People ex rel. Lockyer v. Superior Court* (2004) 122 CA4th 1060, 1079-1080, 19 CR3d 324]. In another case, the court denied the plaintiff's motion to compel a response to a request for production of electronic databases, in part because the defendant had previously produced voluminous hard-copy documents covering the same subject matter [*Jones v. Goord*, 2002 US Dist LEXIS 8707, at *42, *48 (SDNY May 15, 2002)] .

 Cross References:

Discussion of procedure for seeking protective orders, see Ch. 11, Seeking or Opposing Protective Order.

Discussion of objection to request for production of electronically stored information on grounds of inaccessibility due to undue burden or expense, see 10.07[2].



9 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 10 Opposing Demands for Production of Electronic Evidence in California Court
II. DETERMINING WHETHER GROUNDS FOR OBJECTION EXIST

1-10 MB Practice Guide: CA E-Discovery and Evidence 10.08

10.08 Responding Party May Object on Grounds of Confidentiality or Privilege.

10.08[1] Privileged Information Is Outside Scope of Discovery. Electronically stored information that is privileged is outside the permissible scope of discovery [*CCP* § 2017.010; see *CCP* § 2031.010(a); see also *Evid Code* § 900 et seq. (statutory privileges)].



Strategic Point:

The burden of establishing that a particular matter is privileged is on the party asserting that privilege [*San Diego Prof'l Ass'n v. Superior Court* (1962) 58 C2d 194, 199, 23 CR 384, 373 P2d 448]. However, if a privilege is claimed on the ground that the matter sought to be disclosed is a communication made in confidence in the course of the lawyer-client, physician-patient, psychotherapist-patient, clergy-penitent, husband-wife, sexual assault counselor-victim, or domestic violence counselor-victim relationship, a showing that the communication was made between persons in one of those relationships gives rise to a presumption that it was made in confidence. The opponent of the claim of privilege then has the burden of proof to establish that the communication was not confidential [*Evid Code* § 917(a)]. A communication between persons in one of these relationships does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication [*Evid Code* § 917(b)].

Distinguish:

The protection against discovery of attorney work product is not, strictly speaking, an evidentiary privilege, although it is occasionally referred to as such [see, e.g., *Wells Fargo Bank v. Superior Court* (2000) 22 C4th 201, 214-215 & n5, 91 CR2d 716, 990 P2d 591 (explaining "work product doctrine" but at one point referring to "work product privilege")]. However, in the context of discovery demands, most of the same rules apply to attorney work product as to privileged material [see, e.g., *CCP* § 2031.300(a) (failure to raise timely objection to production demand forfeits objections based on privilege and work-product protection)].



Cross Reference:

Discussion of particular privileges, see 10.08[3]-[7].

10.08[2] Privilege May Be Waived or Forfeited. Generally, a claim of privilege concerning electronically stored information can be waived or forfeited in one of three ways:

- Failure to timely object or respond to a request for production of the information [CCP § 2031.300(a)].
- Disclosure or consent to disclosure of the privileged information [Evid Code § 912].
- Placing the privileged matter at issue [see *Venture Law Group v. Superior Court* (2004) 118 CA4th 96, 105, 12 CR3d 656 (attorney-client privilege); *McKesson HBOC, Inc. v. Superior Court* (2004) 115 CA4th 1229, 1239, 9 CR3d 812 (attorney-client privilege and work-product protection)].

Exceptions:

Disclosure by one of two or more joint holders of a privilege does not waive the privilege on behalf of the non-disclosing party [Evid Code § 912(b)]. In addition, a disclosure in confidence of a communication that is protected by the attorney-client, physician-patient, psychotherapist-patient, or sexual assault counselor-victim privilege is not a waiver of that privilege if the disclosure is reasonably necessary to accomplish the purpose of the consultation [Evid Code § 912(d); see *Zurich Am. Ins. Co. v. Superior Court* (2007) 155 CA4th 1485, 1495, 66 CR3d 833 (attorney-client privilege extends to confidential communications between client's agents or employees concerning legal advice and strategy, as long as disclosure to agents and employees is reasonably necessary to further purpose of legal consultation)]. A disclosure that is itself privileged, such as an attorney-client discussion about the client's confidential communication with a psychotherapist, is not a waiver of any privilege [Evid Code § 912(c)].

➡ **Cross References:**

Discussion of moving for relief from forfeiture of objections by reason of late response to production demand, see 10.13.

Forms for use in moving for relief from forfeiture, see 10.15-10.17.

10.08[3] Responding Party Need Not Produce Material Protected by Attorney-Client Privilege. A client, whether or not a party to a particular action, has a privilege to refuse to disclose, and to prevent another from disclosing, a confidential communication between the client and the client's attorney [Evid Code § 954]. The privilege may be asserted by the holder of the privilege and any person authorized by the holder to claim the privilege [Evid Code § 954(a), (b)]. The attorney must claim the privilege unless (1) there is no holder of the privilege in existence, or (2) the attorney is otherwise instructed by a person authorized to permit disclosure [Evid Code §§ 954(c), 955].

➡ **Cross Reference:**

Detailed coverage of attorney-client privilege, see *Matthew Bender(R) Practice Guide: California Civil Discovery*, Ch. 2, 2.16.

10.08[4] Responding Party Need Not Produce Material Protected As Attorney Work Product. Any writing that reflects an attorney's impressions, conclusions, opinions, legal research or theories is not discoverable under any circumstances [CCP § 2018.030(a); see *Wells Fargo Bank v. Superior Court* (2000) 22 C4th 201, 214-215, 91 CR2d 716, 990 P2d 591]. Other attorney work product is subject to qualified protection, and is not discoverable unless the court determines that denial of discovery will unfairly prejudice the party seeking discovery in preparing that party's claim or defense or will result in an injustice [CCP § 2018.030(b)].

 Cross Reference:

Detailed coverage of attorney work-product protection, see *Matthew Bender(R) Practice Guide: California Civil Discovery*, Ch. 2, 2.25-2.32.

10.08[5] Responding Party Need Not Produce Trade Secrets. The owner of a trade secret has a privilege to refuse to disclose the secret and to prevent another from disclosing it, if the allowance of the privilege will not tend to conceal fraud or otherwise work an injustice [*Evid Code* § 1060]. For this purpose, a "trade secret" is information, including a formula, pattern, compilation, program, device, method, technique, or process, that both [*CC* § 3426.1(d)]:

- 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.
- Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Strategic Point--Burden-Shifting:



As with any privilege, the initial burden of establishing the trade secret privilege is on the party asserting that privilege. If that party establishes that the particular matter is a trade secret, the burden then shifts to the party seeking discovery, who must show that the information sought is relevant and necessary to the proof of, or defense against, a material element of one or more causes of action presented in the case, and that it is reasonable to conclude that the information sought is essential to a fair resolution of the lawsuit. It is then up to the holder of the privilege to demonstrate any claimed disadvantages of a protective order. Either party may propose less-intrusive alternatives to disclosure of the trade secret, but the burden is on the trade secret claimant to demonstrate that an alternative to disclosure will not be unduly burdensome to the opposing side and that it will maintain the same fair balance in the litigation that would have been achieved by disclosure [*Bridgestone/Firestone, Inc. v. Superior Court* (1992) 7 CA4th 1384, 1393, 9 CR2d 709] .

Consider:

In practice, trade secrets are often protected by a confidentiality order that is often stipulated to by the parties and entered by the court.

 Cross Reference:

Detailed coverage of trade-secret privilege, see *Matthew Bender(R) Practice Guide: California Civil Discovery*, Ch. 2, 2.24.

10.08[6] Public Entity Need Not Produce Official Information. A public entity may assert a privilege for certain "official information," which is defined as information acquired in confidence by a public employee in the course of his or her duty and not open, or officially disclosed, to the public before the claim of privilege is made [*Evid Code* § 1040(a)]. A similar privilege applies to the identity of an informer who has furnished information in confidence to a law enforcement officer, to a representative of an administrative agency charged with administering or enforcing the law alleged to be violated, or to any person for the purpose of transmittal to a law enforcement officer or representative of an administrative agency [*Evid Code* § 1041(b)]. Generally, the public entity may refuse to disclose official information (including the identity of an informer), and prevent another entity or individual from disclosing it, if either of the following circumstances exists [*Evid Code* §§ 1040(b), 1041(a)]:

- Disclosure is forbidden by a California or federal statute.
- Disclosure is against the public interest because the need to preserve the confidentiality of the

information outweighs the need for disclosure in the public interest. In determining whether disclosure of the information is against the public interest, the interest of the public entity as a party in the outcome of the proceeding in which discovery is sought may not be considered. No privilege may be claimed under this provision, however, if any person authorized to do so has consented that the information be disclosed in the proceeding in which discovery is sought [*Evid Code* §§ 1040(b)(2), 1041(a)(2), (c) (public entity does not have privilege to prevent informer from disclosing own identity)].

 Cross Reference:

Detailed coverage of privilege for official information, see *Matthew Bender(R) Practice Guide: California Civil Discovery*, Ch. 2, 2.23.

10.08[7] Responding Party Need Not Produce Information Protected by Other Privileges. Other constitutional and statutory privileges may be asserted in opposition to a demand for the production of electronically stored information.

Examples:

Constitutional and statutory privileges include the following:

- The constitutional right to privacy [*Cal Const*, art I, § 1; see *TBG Ins. Servs. Corp. v. Superior Court* (2002) 96 CA4th 443, 450-452, 117 CR2d 155 (employee had diminished expectation of privacy in data found on company-owned computer he kept at home, because he agreed to allow company to inspect computer at any time)].
- The constitutional privilege against self-incrimination [*US Const amend VI*].
- The privilege for confidential marital communications [*Evid Code* § 980 *et seq.*].
- The physician-patient privilege [*Evid Code* § 990 *et seq.*].
- The psychotherapist-patient privilege [*Evid Code* § 1010 *et seq.*].
- The clergy-penitent privilege [*Evid Code* § 1030 *et seq.*].
- The sexual assault counselor-victim privilege [*Evid Code* § 1035 *et seq.*].
- The domestic violence counselor-victim privilege [*Evid Code* § 1037 *et seq.*].
- The human trafficking case worker-victim privilege [*Evid Code* § 1038 *et seq.*].

 Cross Reference:

Discussion of miscellaneous privileges, see *Matthew Bender(R) Practice Guide: California Civil Discovery*, Ch. 2, *Scope of Discovery*, 2.42- 2.51.



10 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 10 Opposing Demands for Production of Electronic Evidence in California Court

III. ASSERTING OBJECTIONS TO PRODUCTION DEMANDS

1-10 MB Practice Guide: CA E-Discovery and Evidence 10.09

10.09 CHECKLIST: Asserting Objections to Production Demands.

☐ If any particular demand for production of electronically stored information is objectionable, determine manner of asserting objection, either:

☐ In formal response to demand.

Authority:

CCP § 2031.240(b)

Discussion:

See 10.11

☐ By motion for protective order.

Authority:

CCP § 2031.060

Discussion:

See 10.12

☐ If asserting objection in formal response to demand:

☐ Ensure that objection includes all of following:

Authority:

CCP § 2031.240(b)

Discussion:

See 10.11[1]

Form:

See *Ch. 8, Responding to Electronic Discovery Demands in California Courts*, 8.24

☐ Identification of item or category of information to which objection is made.

☐ Statement of reason or grounds for objection, expressly identifying particular privilege or work-product protection, if applicable.

☐ If objection is based on claim that electronically stored information is from source that is not reasonably accessible, both of following:

Authority:

CCP § 2031.210(d)

☐ Statement that responding party will not search source in absence of agreement with demanding party or court order.

☐ Identification of types or categories of sources of electronically stored information that are not reasonably accessible.

☐ Follow standard procedures for responding to production demand.

Standard Procedure Checklist:

See *Ch. 8, Responding to Electronic Discovery Demands in California Court*, 8.12.

☐ If asserting objection by motion for protective order:

☐ Meet and confer with opposing counsel to resolve objections informally before filing motion for protective order.

Authority:

CCP §§ 2016.040, 2031.060(a)

Discussion:

See 10.12[1]

☐ Follow standard procedures for making motion for protective order.

Standard Procedure Checklist:

See *Ch. 11, Seeking or Opposing Protective Order*, 11.03.

☐ If timely response to production demand was not filed, seek relief from forfeiture of objections.

Authority:

CCP § 2031.300(a)

Discussion:

See 10.13

Forms:

See 10.15-10.17

☐ Prepare and serve response that complies with all applicable statutory requirements other than timeliness.

Standard Procedure Checklist:

See *Ch. 8, Responding to Electronic Discovery Demands in California Court*, 8.12.

☐ Ascertain facts demonstrating that failure to serve timely response was result of mistake, inadvertence, or excusable neglect.

☐ Move for relief from forfeiture of objections, following standard procedure for noticed motion.

Cross Reference:

Standard format for noticed motion, see *Matthew Bender Practice Guide: California Pre-Trial Civil Procedure*, Ch. 26, 26.39-26.45.

☐ If privileged information has been inadvertently produced in response to demand:

Authority:

CCP § 2031.285(a)

Discussion:

See 10.14

☐ Notify every party that received information of claim of privilege and basis for claim.

☐ If demanding party moves for determination of privilege claim, oppose motion.



11 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 10 Opposing Demands for Production of Electronic Evidence in California Court

III. ASSERTING OBJECTIONS TO PRODUCTION DEMANDS

*1-10 MB Practice Guide: CA E-Discovery and Evidence 10.10***10.10 Options and Strategies.**

Once counsel has determined that one or more items in a demand for production of electronically stored information is objectionable, counsel must decide whether to seek a protective order, or to assert the objections in the response to the demand and wait for a motion to compel a further response [see CCP §§ 2031.060(a), 2031.210, 2031.310]. As the moving party seeking a protective order, the responding party will have the first chance to frame the discovery issues. On the other hand, asserting objections in the response to the demand may conserve resources and court time, because the demanding party might decide not to move to compel a further response [see CCP § 2031.310(c) (failure to move for further response within 45 days after service of response generally forfeits right to compel further response)].

 Cross References:

Discussion of asserting objections in response to demand, see 10.11.

Discussion of asserting objections by moving for protective order, see 10.12

 Warning:

Both courses of action--moving for a protective order, or raising objections in the response--run the risk of incurring sanctions. The court generally must award sanctions against the losing party on a motion for a protective order and a motion to compel a further response [CCP §§ 2031.060(h), 2031.300(h)].

 Cross References:

Discussion of seeking or opposing sanctions in connection with protective order, see Ch. 11, Seeking or Opposing Protective Order

Discussion of seeking or opposing sanctions in connection with motion to compel, see Ch. 12, *Seeking or Opposing Motion to Compel*, 12.07, 12.12, 12.17, 12.22, 12.27, 12.31.

Discussion of seeking or opposing sanctions for noncompliance with demand for production, see Ch. 13, Seeking or Opposing Sanctions for Noncompliance.

A failure to timely object or respond to a request for production ordinarily will result in the forfeiture of any objections, including those based on privilege or work-product protection [CCP § 2031.300(a)]. If the response deadline has been

missed because of mistake, inadvertence, or excusable neglect, counsel should promptly serve a response, including objections, and move the court for an order granting relief from the forfeiture [see *CCP* § 2031.300(a)].

➡ **Cross References:**

Discussion of motion for relief from forfeiture of objections, see *10.13*.

Forms, see *10.15-10.17*.

If electronically stored information subject to a claim of privilege has been inadvertently disclosed in response to a production demand, counsel should immediately notify all parties that received the inadvertent disclosure of the claim of privilege [see *CCP* § 2031.285].

➡ **Cross Reference:**

Discussion of procedure for return of inadvertently disclosed information, see *10.14*.



12 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 10 Opposing Demands for Production of Electronic Evidence in California Court

III. ASSERTING OBJECTIONS TO PRODUCTION DEMANDS

1-10 MB Practice Guide: CA E-Discovery and Evidence 10.11

10.11 Responding Party May Assert Objections in Response to Demand.

10.11[1] Response Should Comply With Formal Requirements. A responding party may assert objections to a demand for production of electronically stored information in a formal response to the demand [CCP § 2031.240(b)]. Each objection must identify the item or category to which the objection is made, and it must expressly state the reason or grounds for the objection [CCP § 2031.240(b)].

If the objection is based on a claim of privilege, the particular privilege must be identified [see CCP § 2031.240(b)(2)]. If an objection is based on a claim that the information sought is protected work product [see CCP § 2018.010 *et seq.*], that claim must be expressly asserted [see CCP § 2031.240(b)(2)].



Strategic Point:

Courts tend to frown upon blanket objections. Therefore, instead of simply objecting to a particular demand as vague, overly broad, or not stated with reasonable particularity, counsel should consider including a statement that the responding party will comply with the request to a more limited or narrow extent. In other words, state the objection and follow it with a statement that the responding party intends to partially comply by providing a more limited or narrowly focused category of information. Then specifically identify the category that will be produced.

If the responding party objects to the discovery of electronically stored information on the grounds that it is from a source that is not reasonably accessible because of undue burden or expense, the objection must include all of the following [CCP § 2031.210(d)]:

- A statement that the responding party will not search the source in the absence of an agreement with the demanding party or court order.
- Identification of the types or categories of sources of electronically stored information that the responding party asserts are not reasonably accessible.

By objecting and identifying the type or category of sources of information that are not reasonably accessible, the

responding party preserves any other objections it may have to the information specified in the objection [CCP § 2031.210(d)].



Timing:

A response to a demand for production must be served within 30 days after service of the demand (five days after service of the demand, in an unlawful detainer action), unless the court has shortened or extended the time to respond or the parties have agreed in writing to an extended date for serving a response [CCP §§ 2031.260, 2031.270]. A failure to timely object or respond to a request for production ordinarily will result in the forfeiture of any objections, including those based on privilege or work-product protection [CCP § 2031.300(a)].



Cross References:

Discussion of objection based on inaccessibility of source of electronically stored information, see 10.07[2].

Discussion of objections based on privilege or work-product protection, see 10.08[3], [4].

Discussion of motion for relief from forfeiture of objections, see 10.13.

Discussion of generally applicable procedures for responding to production demand, including forms, see Ch. 8, Responding to Electronic Discovery Demands in California Court.

10.11[2] Privilege Log Need Not Be Prepared Unless Demanding Party Moves to Compel. A privilege log is a specific factual description of documents created to substantiate a claim of privilege for documents withheld in connection with a request for document production. The response to the demand for production need not include a privilege log. Rather, the responding party must prepare a privilege log only if the court orders it in connection with a motion to compel a further response to the demand [*People ex rel. Lockyer v. Superior Court* (2004) 122 CA4th 1060, 1075, 19 CR3d 324 ; *Best Prods., Inc. v. Superior Court* (2004) 119 CA4th 1181, 1189, 15 CR3d 154 (purpose of providing privilege log is to permit judicial evaluation of claim of privilege)].

Failure to provide a privilege log to the party propounding a demand for production does not waive privilege under state court practice [*Best Products v. Superior Ct.* (2004) 119 CA4th 1181, 1188 15 CR3d 154 (privilege log is not required with response, and not relevant until after the propounding party challenges a claim of privilege)].



Strategic Points--Responding Party:

Although it is not required to accompany the response to the production demand, it is a good idea to prepare a privilege log, because the court can ask for specifics on a motion to compel concerning the basis for asserting a privilege [see *Best Prods., Inc. v. Superior Court* (2004) 119 CA4th 1181, 1189, 15 CR3d 154] . If it becomes necessary to prepare a privilege log, counsel should seek a stipulation that the log need not list any communications that occurred solely between client and counsel after the client filed the complaint or was served with the summons. Listing all such communications would be burdensome, and it is unlikely that any communications between client and counsel would not be subject to a legitimate claim of privilege.



Cross References:

Discussion of objections based on privileges, see 10.08. Procedures for preparation of privilege log, see Ch 9, *Gathering and Producing Electronically Stored Evidence*, 9.46.

Discussion of privileges, see *Matthew Bender(R) Practice Guide: California Civil Discovery*, Ch. 2, § 2.09-§ 2.24, § 2.42-§ 2.51.

Discussion of motion to compel further response, see Ch. 12, *Obtaining or Opposing Motion to Compel*, 12.13-12.17.

10.11[3] Demanding Party May Move for Further Response. If the responding party asserts objections in a response to the demand for production of electronically stored information and does not move for a protective order or other order limiting discovery, the demanding party may move for an order compelling a further response [*CCP* § 2031.310(a)(3)].



Cross Reference:

Discussion of making and opposing motion to compel further response, see Ch. 12, *Obtaining or Opposing Motion to Compel*, 12.13-12.17.



13 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 10 Opposing Demands for Production of Electronic Evidence in California Court

III. ASSERTING OBJECTIONS TO PRODUCTION DEMANDS

1-10 MB Practice Guide: CA E-Discovery and Evidence 10.12

10.12 Responding Party May Seek Protective Order.

10.12[1] Objection May Be Asserted in Motion for Protective Order. On receiving a demand for the production of electronically stored information, the responding party may opt to move for a protective order, rather than respond with an objection and wait for a motion to compel a further response [see *CCP* §§ 2031.060(a), 2031.210, 2031.310]. As the moving party seeking a protective order, the responding party will have the first chance to frame the discovery issues.

Prerequisite:

Before moving for a protective order, counsel must make a good-faith attempt at informal resolution of the objection through a meeting and conference with opposing counsel (sometimes called a "meet and confer") [*CCP* §§ 2016.040, 2031.060(a)]. A declaration of attempts to meet and confer must be filed with the motion [*CCP* § 2031.060(a)].



Cross Reference:

Discussion of seeking and opposing protective orders, see Ch. 11, Seeking or Opposing Protective Order.



Timing:

Although the statute governing protective orders requires only that a motion be made "promptly" [see *CCP* § 2031.060(a)], counsel for the responding party should ensure that objections are asserted--either by moving for a protective order or serving a response to the production demand--no later than 30 days after service of the demand. Waiting longer than 30 days (five days in an unlawful detainer case) will result in the forfeiture of any objections, including those based on privilege or work-product protection [*CCP* § 2031.300(a); see *CCP* § 2031.260].



Cross References:

Discussion of timing of response to production demand, see 10.11[1].

Discussion of motion for relief from forfeiture of objections, see 10.13.

Discussion of generally applicable procedures for responding to production demand, including forms, see Ch. 8, Responding to Electronic Discovery Demands in California Court.

10.12[2] Court May Issue Protective Order on Ground That Information Is Inaccessible or on Other Traditional Grounds. The court may issue a protective order on any of four traditional bases: unwarranted annoyance, embarrassment, oppression, or undue burden or expense [CCP § 2031.060(b); *see also* CCP § 2017.020(a)]. The most frequently urged basis for a protective order against a demand for electronically stored information is that the information is not reasonably accessible because of undue burden or expense [*see* CCP § 2031.060(b)-(f)].

Cross References:

Discussion of electronically stored information that is not reasonably accessible, see 10.07[2].

Discussion of protective orders against demands for production of electronically stored information, see Ch. 11, Seeking or Opposing Protective Order.

Discussion of protective orders generally, see *Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 1, Strategy and Planning, §1.15, §1.16* (Matthew Bender).

10.12[3] Court Has Broad Power to Tailor Protective Order. The court has broad powers to issue protective orders: it may make "any order that justice requires" to protect the parties from these discovery abuses [CCP § 2031.060(b)]. A protective order may flatly deny discovery of the electronically stored information sought, or it may allow discovery but reduce or mitigate the production challenges faced by the responding party, by directing the parties to take different actions than those originally specified in the discovery demand [*see* CCP § 2031.060(b)].

Examples:

A protective order may include, but is not limited to, any of the following directions [CCP § 2031.060(b)]:

- That all or some of the information demanded need not be produced or made available at all.
- That the time for a response to a set of demands, or to a particular item or category in the set of demands be extended.
- That the place of production be other than that specified in the demand.
- That the inspection, copying, testing, or sampling be made only on specified terms and conditions.
- That a trade secret or other confidential research, development, or commercial information not be disclosed, or be disclosed only to specified persons or only in a specified way.
- That the items produced be sealed and thereafter opened only on order of the court.

10.12[4] Even If Court Orders Discovery, It May Impose Conditions and Allocate Costs. If the court finds good cause for the production of electronically stored information from a source that is not reasonably accessible, the court may allocate the expense of discovery and set other discovery conditions [CCP § 2031.060(d), (e); *see* CCP § 1985.8(f) (applicable when nonparty opposes subpoena for electronically stored information)].

Consider:

To lessen the burden of discovery, counsel may suggest to the court such conditions as sampling or testing of a given source of electronically stored information, rather than full production [*see Hill v.*

Eddie Bauer (CD Cal 2007) 242 FRD 556, 564 (allowing sampling, because full response to demand would have been unduly burdensome)]; scheduling production of demanded information in stages; or requiring production in a format that is less expensive than the format specified in the discovery demand.

Distinguish--Mandatory Cost-Shifting for "Translation":

If translation of any data compilations included in the demand is necessary to put the demanded information in a reasonably usable form, the responding party, using "detection devices," must translate the information, and the demanding party must pay the reasonable expense of that translation [*CCP § 2031.280(e)*; *Toshiba Am. Elec. Components, Inc. v. Superior Court* (2004) 124 CA4th 762, 769-772, 21 CR3d 532 (cost-shifting under substantially identical predecessor of *CCP § 2031.280(e)* is mandatory); see also *CCP § 1985.8(g)* (similar requirement when nonparty is subpoenaed to produce electronically stored information)].

 Cross Reference:

Discussion of orders allocating expenses and setting conditions for discovery, see *Ch. 11, Seeking or Opposing Protective Order, 11.12[1], 11.19*.

10.12[5] Even If Protective Order Is Denied, Court Must Limit Frequency or Extent of Cumulative or Burdensome Discovery. Even if the court denies a motion for a protective order, it must limit the frequency or extent of discovery of electronically stored information if, under the conditions, the demanded discovery is cumulative or burdensome [*CCP § 2031.060(f)*; see *CCP § 1985.8(h)* (applicable when nonparty opposes subpoena for electronically stored information)]. This requirement applies even if the court finds that the source of the information is reasonably accessible or that there is good cause for discovery of information that is not reasonably accessible [*CCP § 2031.060(d), (f)*; see *CCP § 1985.8(e), (h)* (applicable when nonparty is subpoenaed to produce electronically stored information)].

 Cross References:

Discussion of conditions that require court to issue order limiting frequency or extent of discovery, see *10.07[3]*.

Discussion of procedures for obtaining order limiting frequency or extent of discovery, see *Ch. 11, Seeking or Opposing Protective Order, 11.19*.



14 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 10 Opposing Demands for Production of Electronic Evidence in California Court

III. ASSERTING OBJECTIONS TO PRODUCTION DEMANDS

1-10 MB Practice Guide: CA E-Discovery and Evidence 10.13

10.13 Responding Party May Move for Relief From Forfeiture of Objections After Failure to Serve Timely Response.

The responding party's failure to serve a timely response to a demand for production of electronically stored information ordinarily works a forfeiture (called "waiver" in the statute) of any objection to the demand, including one based on privilege or on work product protection [CCP § 2031.300(a)]. However, the court may relieve the responding party from the forfeiture if it determines that both of the following conditions have been satisfied [CCP § 2031.300(a)]:

- The responding party has subsequently served a response that is in substantial compliance with applicable statutory requirements [see CCP §§ 2031.210-2031.240, 2031.280].
- The responding party's failure to serve a timely response was the result of mistake, inadvertence, or excusable neglect.

In deciding whether a failure to serve a timely response was the result of mistake, inadvertence, or excusable neglect, the court will apply the same standard as that used in determining whether to grant relief from judgment under CCP § 473(b) [*City of Fresno v. Superior Court* (1988) 205 CA3d 1459, 1467, 253 CR 296] .

Examples--Relief Not Justified:

- Counsel's mistake of law on a relatively simple and undebatable matter is not a valid ground for relief, nor is the fact that counsel is very busy [*City of Fresno v. Superior Court* (1988) 205 CA3d 1459, 1467, 253 CR 296] .
- A tactical choice made by counsel does not constitute mistake, inadvertence, or excusable neglect. Thus, counsel's failure to assert the attorney-client privilege in response to one party's production demand, in reliance on potential relief from an ultimately unsuccessful motion for a protective order against discovery sought by another party, was deemed a tactical choice to pursue a certain course of action, rather than a mistake or excusable neglect [*Scottsdale Ins. Co. v. Superior Court* (1997) 59 CA4th 263, 274-276, 69 CR2d 112] .

 Cross Reference:

Forms for motion for relief from forfeiture of objections, see *10.15-10.17*.



15 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 10 Opposing Demands for Production of Electronic Evidence in California Court

III. ASSERTING OBJECTIONS TO PRODUCTION DEMANDS

*1-10 MB Practice Guide: CA E-Discovery and Evidence 10.14***10.14 Responding Party May Seek Return of Inadvertently Disclosed Privileged Material.**

If electronically stored information produced in discovery is subject to a claim of privilege or work-product protection, the responding party may notify any party that received the information of the claim of privilege and the basis for the claim [CCP § 2031.285(a)].

After being notified, the demanding party must immediately sequester the specified information and either (1) return the information and any copies that may exist, or (2) present the information to the court conditionally under seal for a determination of the privilege or work-product claim [CCP § 2031.285(b)]. If the information is presented to the court under seal, the demanding party then has 30 days to make a motion for determination of the claim of privilege or work-product protection [CCP § 2031.285(d)(1)].

Until the legitimacy of the claim of privilege or protection is resolved, the demanding party must preserve the information and keep it confidential, and may not use the information in any manner [CCP § 2031.285(c)(1), (d)(2)]. If the demanding party disclosed any of the information before receiving notice of the claim of privilege or protection, the demanding party must take reasonable steps to retrieve the information after receiving notice of the claim [CCP § 2031.285(c)(2)].

**Warning--Demanding Party:**

Even in the absence of notification that privileged or protected material has been inadvertently produced, counsel has an ethical duty to honor the confidential nature of the material. When an attorney receives materials that are clearly confidential and privileged, and it is reasonably apparent that they were inadvertently disclosed, that attorney must refrain from further examining the material and immediately notify the provider that he or she possesses materials that appear to be privileged. The attorney must also notify the party entitled to the privilege [see *Rico v. Mitsubishi Motors Corp.* (2007) 42 C4th 807, 817, 68 CR3d 758, 171 P3d 1092 ; *State Comp. Ins. Fund v. WPS, Inc.* (1999) 70 CA4th 644, 652-654, 82 CR2d 799] .

**Cross Reference:**

Detailed coverage of handling of inadvertently disclosed information that is privileged or protected as work product, see *Ch. 3, Ethical Issues for Attorneys in E-Discovery*, 3.14-3.15.



16 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 10 Opposing Demands for Production of Electronic Evidence in California Court
IV. FORMS

1-10 MB Practice Guide: CA E-Discovery and Evidence 10.15

10.15 Notice of Motion and Motion for Relief From Waiver of Objections to Demand for Production of Electronically Stored Information.

Notice of Motion and Motion for Relief From Waiver of Objections to Demand for Production of Electronically Stored Information.

Jane Lee

California Bar Number 123456

50 South Main St., Suite 100

Farallon City, California 90000

Phone: 555-999-9999

Attorney for Defendant, Mary Jones Enterprises, Inc.

SUPERIOR COURT OF CALIFORNIA,

COUNTY OF FARALLON

	)	
	)	No. _____
	)	NOTICE OF MOTION AND MOTION
	)	FOR RELIEF FROM
	)	WAIVER OF OBJECTIONS
John Smith, Plaintiff, vs. Mary Jones Enterprises,	)	Date: _____
Inc., Defendant.	)	Time: _____
	)	Location: _____
	)	Judge: _____
	)	Date Action Filed: _____
	)	Trial Date: _____
	)	

To Plaintiff, John Smith, and his attorney of record:

NOTICE IS HEREBY GIVEN that, on _____ [date], at _____ [time], or as soon thereafter as the matter may be heard, in [_____ (Department or Division) _____ of]

this court, located at 1 North Main Street, Farallon City, California, Defendant, Mary Jones Enterprises, Inc., will, and hereby does, move for an order relieving Defendant from the forfeiture or waiver of objections to Plaintiff's First Set of Demands for Production of Electronically Stored Information.

The motion is made pursuant to *Code of Civil Procedure Section 2031.300(a)*, on the grounds that on _____ [date]. Defendant served a response that is in substantial compliance with the requirements of *Code of Civil Procedure Sections 2031.210-2031.240* and *2031.280*, and that Defendant's failure to serve a timely response was the result of mistake, inadvertence, or excusable neglect. The motion is based on this notice of motion, the accompanying declaration(s) of _____ [name(s)], the accompanying supporting memorandum, the records and file herein, and such evidence as may be presented at the hearing on the motion.

Dated: _____

Respectfully submitted,

_____ [signature]

Jane Lee

Attorney for Defendant, Mary Jones Enterprises, Inc.

NOTES:

Authority:

CCP § 2031.300(a)

Checklist:

See 10.09

Discussion:

See 10.13

Related Form for Declaration Supporting Motion:

See 10.16

Related Form for Order:

See 10.17



17 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

IV. FORMS

1-10 MB Practice Guide: CA E-Discovery and Evidence 10.16

10.16 Declaration of Counsel in Support of Motion for Relief From Waiver of Objections to Demand for Production of Electronically Stored Information.

Declaration of Counsel in Support of Motion for Relief From Waiver of Objections to Demand for Production of Electronically Stored Information.

Jane Lee

California Bar Number 123456

50 South Main St., Suite 100

Farallon City, California 90000

Phone: 555-999-9999

Attorney for Defendant, Mary Jones Enterprises, Inc.

SUPERIOR COURT OF CALIFORNIA,

COUNTY OF FARALLON

John Smith, Plaintiff, vs. Mary Jones Enterprises,
Inc., Defendant.

$$\begin{array}{c}) \\) \\) \\) \\) \\) \\) \\) \\) \\) \end{array}$$

No. _____

DECLARATION OF MOTION

FOR RELIEF FROM

WAIVER OF OBJECTIONS

Date: _____

Time:

Location: _____

Judge: _____

Date Action Filed: _____

Trial Date: _____

To Plaintiff, John Smith, and his attorney of record:

NOTICE IS HEREBY GIVEN that, on _____ [date], at _____ [time], or as soon

thereafter as the matter may be heard, in [_____] (Department or Division) _____ of] this court, located at 1 North Main Street, Farallon City, California, Defendant, Mary Jones Enterprises, Inc., will, and hereby does, move for an order relieving Defendant from the forfeiture or waiver of objections to Plaintiff's First Set of Demands for Production of Electronically Stored Information.

I, Jane Lee, declare:

1. I am an attorney at law duly admitted to practice before all the courts of the State of California and the attorney of record in this action for Defendant, Mary Jones Enterprises, Inc.
2. On _____ [date], Plaintiff, John Smith, served Plaintiff's First Set of Demands for Production of Electronically Stored Information on Defendant by _____ [identify method of service, e.g. , personal service or U.S. Mail or courier]. Pursuant to *Code of Civil Procedure Section 2031*, Defendant's response to the demand was due on _____ [date].
3. _____ [State facts showing grounds for late response due to mistake, inadvertence, or excusable neglect].
4. Defendant did serve a response on Plaintiff by _____ [identify method of service, e.g. , personal service or U.S. Mail or courier] on _____ [date]. Defendant's response includes objections to Item No. 1 and Item No. 2 of the demand. A true and correct copy of Defendant's response is attached as Exhibit A.
5. Defendant seeks an order from this Court granting relief from forfeiture or waiver of its objections to Item No. 1 and Item No. 2 of the demand.
6. On _____ [date], I _____ [specify actions taken to meet and confer with opposing party in a reasonable, good-faith attempt to reach informal resolution of the issues presented by the motion, e.g., conferred with Plaintiff's counsel by telephone and requested that Plaintiff honor late objections, and we were unable to resolve the issues presented by this motion].

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct of my own personal knowledge.

Dated: _____
 _____ [signature]

Jane Lee
 Attorney for Defendant, Mary Jones Enterprises, Inc.

NOTES:

Authority:

CCP § 2031.300(a)

Checklist:

See 10.09

Discussion:

See 10.13

Related Form for Notice of Motion and Motion:

See 10.15

Related Form for Order:

See *10.17*



18 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 10 Opposing Demands for Production of Electronic Evidence in California Court
IV. FORMS*1-10 MB Practice Guide: CA E-Discovery and Evidence 10.17***10.17 Order Granting Relief From Waiver of Objections to Demand for Production of Electronically Stored Information.**Order Granting Relief From Waiver of Objections to Demand for Production of Electronically Stored Information.
SUPERIOR COURT OF CALIFORNIA,
COUNTY OF FARALLON

John Smith, Plaintiff, vs. Mary Jones Enterprises,	)	No. _____
Inc., Defendant.	)	ORDER GRANTING RELIEF FROM WAIVER OF
	)	OBJECTIONS

The motion of Defendant, Mary Jones Enterprises, Inc., for an order relieving Defendant from the forfeiture or waiver of objections to Plaintiff's First Set of Demands for Production of Electronically Stored Information came on regularly for hearing by the Court on _____ [date]. Defendant appeared by counsel Jane Lee; Plaintiff appeared by counsel Tom Doe.

The Court, having considered the declarations and other documents in support of and in opposition to the motion, having heard the arguments of counsel, and being fully advised in the matter, finds as follows:

1. Defendant's failure to serve a timely response to Plaintiff's First Set of Demands for Production of Electronically Stored Information was the result of excusable neglect.
2. On _____ [date], Defendant served a response to Plaintiff's First Set of Demands for Production of Electronically Stored Information that, aside from being late, complied with applicable statutory requirements.

IT IS THEREFORE ORDERED that the motion be, and hereby is, granted, and that any objections asserted in Defendant's response to Plaintiff's First Set of Demands for Production of Electronically Stored Information are not forfeited or waived.

Dated: _____

_____ [signature]
Judge of the Superior Court

NOTES:

Authority:

CCP § 2031.300(a)

Checklist:

See 10.09

Discussion:

See 10.13

Related Form for Motion and Notice of Motion:

See 10.15

Related Declaration:

See 10.16



19 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 11 Seeking or Opposing Protective Order

1-11 MB Practice Guide: CA E-Discovery and Evidence 11.syn

§ 11.syn Synopsis to Chapter 11: Seeking or Opposing Protective Order

11.01 Scope.

11.02 Objective and Strategy.

11.03 CHECKLIST: Seeking Protective Order Against Demand for Electronically Stored Information.

11.04 Options and Strategies.

11.05 Protective Order May Issue If Demanded Electronic Discovery Creates Undue Burden or Expense.

11.06 Responding Party Must Demonstrate That Source Is Not Reasonably Accessible.

11.06[1] Responding Party Has Burden of Persuasion.

11.06[2] Source May Be Not Reasonably Accessible If Information Is Not Readily Usable.

11.06[3] Court May for Good Cause Order Discovery of Inaccessible Information.

11.07 Court Has Broad Power to Make Protective Orders.

11.07[1] Protective Orders Are Designed To Prevent Discovery Abuses.

11.07[2] Protective Order Need Not Deny Demanded Discovery.

11.08 CHECKLIST: Opposing Motion for Protective Order.

11.09 Options and Strategies.

11.10 Demanding Party May Demonstrate That Electronic Information Is Reasonably Accessible.

11.11 Demanding Party May Obtain Discovery of Information That Is Not Reasonably Accessible by Demonstrating Good Cause.

11.11[1] Showing of Good Cause May Overcome Finding That Information Is Not Reasonably Accessible.

11.11[2] Court May Consider Several Factors in Determining Good Cause.

11.11[3] Court May Order Sampling or Testing to Aid in Determining Existence of Good Cause for Discovery.

11.12 Court May Set Conditions for Discovery After Finding Good Cause.

11.12[1] Court May Set Conditions and Allocate Discovery Expenses.

11.12[2] Demanding Party Must Pay Cost of Translating Data Compilations.

11.12[3] Court May Shift Significant or Special Costs When Inaccessible Information Is Sought.

11.13 CHECKLIST: Avoiding Monetary Sanctions for Seeking or Opposing Protective Order.

11.14 Options and Strategies.

11.15 Losing Party May Avoid Monetary Sanctions.

11.15[1] Losing Party May Avoid Sanctions by Showing Substantial Justification for Losing Position.

11.15[2] Losing Party May Avoid Sanctions by Showing That Imposition of Sanctions Would Be Unjust.

11.15[3] Losing Party May Avoid Sanctions by Showing That Information Was Lost in Good Faith.

11.16 CHECKLIST: Obtaining Alternative Relief When Motion for Protective Order Is Denied.

11.17 Options and Strategies.

11.18 Court Has Discretion to Set Just Terms and Conditions for Discovery, Including Allocation of Expenses.

11.19 Court Must Limit Frequency or Extent of Discovery of Electronically Stored Information Under Some Circumstances.

11.19[1] Limiting Order May Be Required Even If Protective Order Is Denied.

11.19[2] Responding Party May Obtain Limiting Order by Showing Information Is Available From More Convenient Source.

11.19[3] Responding Party May Obtain Limiting Order by Showing Discovery Sought Is Unreasonably Cumulative or Duplicative.

11.19[4] Responding Party May Obtain Alternative Relief by Showing That Demanding Party Wasted Previous Opportunity for Discovery.

11.19[5] Responding Party May Obtain Alternative Relief by Showing That Burden or Expense of Discovery Outweighs Benefit.

11.20 Notice of Motion and Motion for Protective Order.

11.21 Declaration Supporting Motion for Protective Order.

11.22 Protective Order.



20 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 11 Seeking or Opposing Protective Order

I. STRATEGY

1-11 MB Practice Guide: CA E-Discovery and Evidence 11.01

11.01 Scope.

This chapter covers:

- Obtaining protective orders relating to the discovery of electronically stored information [see 11.03-11.07; *Forms*: 11.20-11.22].
- Opposing protective orders relating to the discovery of electronically stored information [see 11.08-11.12].
- The mandatory imposition of monetary sanctions against the losing party, and exceptions to that requirement [see 11.13-11.15; *Forms*: 11.20, 11.22].
- Obtaining alternative relief when a motion for a protective order is denied [see 11.16-11.19].

Throughout this chapter, the terms "responding party" or "respondent" refer to the party to whom a discovery demand is directed, and the term includes the moving party on a motion for a protective order. "Demanding party" refers to the party who propounds a discovery demand, and the term includes the respondent or opposing party on a motion for a protective order.

Core Statute:

CCP § 2031.060



21 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 11 Seeking or Opposing Protective Order
I. STRATEGY

1-11 MB Practice Guide: CA E-Discovery and Evidence 11.02

11.02 Objective and Strategy.

A demand for the discovery of electronically stored information may place a substantial burden on the respondent in terms of labor, expense, exposure of private or confidential materials, and interference with normal business activities. For this reason, a party who has received a demand for the discovery of electronically stored information may seek to limit the scope and extent of discovery, or oppose such discovery entirely. One method of limiting the scope of discovery is to file a motion for a protective order [see *CCP § 2031.060(a)*].

The court has broad discretion to issue any order that justice requires to protect any party or other person from unwarranted annoyance, embarrassment, or oppression, or undue burden and expense [*CCP § 2031.060(b)*].

If the court finds good cause for production of electronically stored information, despite a finding that the demand is burdensome or expensive for the responding party, it may set conditions and allocate the expenses of electronic discovery [*CCP § 2031.060(e)*]. If the court denies the motion for a protective order, it may order electronic discovery on terms and conditions as are just [*CCP § 2031.060(g)*]. Monetary sanctions must be imposed on the party that loses the motion for a protective order, unless the court finds that that party acted with substantial justification or that other circumstances make the imposition of sanctions unjust [*CCP § 2031.060(h)*].



Strategic Point:

Moving for a protective order is merely one option for the party responding to a demand for production of electronically stored information. The responding party may opt to move for a protective order to accelerate resolution of an issue and to have the opportunity to frame the issues for the court in the first instance, rather than wait for a motion to compel. Alternatively, the responding party can take a defensive approach by objecting to the electronic discovery demand and opposing any subsequent motion to compel.



Cross References:

Discussion of planning e-discovery, see *Ch. 4, Planning E-Discovery, 4.03-4.10*.

Discussion of the procedures for demanding production of electronically stored information, see *Ch. 6, Demanding Production of Electronically Stored Information in California Court, 6.09-6.13*.

Discussion of responding to electronic discovery demand in California court, see *Ch. 8, Responding to Electronic Discovery Requests in California Court*, 8.12-8.23.

Discussion of grounds and procedure for obtaining a protective order, see 11.03-11.07.

Discussion of opposing a protective order, see 11.08-11.12.

Discussion of court-imposed limits on frequency and extent of discovery, see 11.19 and *Ch 10, Opposing Demands for Production of Electronic Evidence in California Court*, 10.12[5].

Discussion of alternative options for responding party, see 11.16-11.19 and *Ch. 8, Responding to Electronic Discovery Requests in California Court*, 8.07.

Discussion of procedures for making or opposing motion to compel a response or a further response to a demand for production, or a motion to compel compliance with a demand for production, see *Ch. 12, Obtaining or Opposing Motion to Compel*.

Discussion of procedures for seeking or opposing sanctions for noncompliance with production demand, see *Ch. 13, Seeking or Opposing Sanctions for Noncompliance*, 13.11-13.15.



22 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 11 Seeking or Opposing Protective Order

II. SEEKING PROTECTIVE ORDER AGAINST DEMAND FOR ELECTRONICALLY STORED INFORMATION

1-11 MB Practice Guide: CA E-Discovery and Evidence 11.03

11.03 CHECKLIST: Seeking Protective Order Against Demand for Electronically Stored Information.

- ☐ Review demand for discovery of electronically stored information promptly after receiving it, to determine whether protective order may be appropriate.

Authority:

CCP § 2031.060(a)

Discussion:

See 11.04, 11.05

- ☐ Consider whether compliance with demand would cause unwarranted annoyance, embarrassment, oppression, or undue burden or expense.

Authority:

CCP § 2031.060(b)

Discussion:

See 11.05.

- ☐ Consider whether demanded electronically stored information is from source that is not reasonably accessible.

Authority:

CCP § 2031.060(c)

Discussion:

See 11.06.

- ☐ Consider whether to assert objections in response to demand as alternative to motion for protective order.

Authority:

CCP § 2031.210(d)

Discussion:

See 11.05

- ☐ Meet and confer with opposing counsel to resolve dispute informally before filing motion for protective order.

Authority:

CCP §§ 2016.040, 2031.060(a)

Discussion:

See 11.04

- ☐ If meet-and-confer does not resolve dispute, prepare necessary documents for motion for protective order.

- ☐ Prepare notice of motion and motion for protective order and request for monetary sanctions.

- ☐ If desired, include request for alternative relief should court deny protective order
[see *CCP § 2031.060(d)-(f)*].

Authority:

CCP § 2031.060(a), (b); Cal Rules Ct, Rule 3.1112(a)(1), (2)

Discussion:

See 11.06, 11.07; 11.17-11.19

Form:

See 11.20

- ☐ Prepare memorandum in support of motion.

Authority:

Cal Rules Ct, Rules 3.1112(a)(3), 3.1113

- ☐ Prepare affidavits or declarations, including expert declarations, along with any appropriate exhibits, that are necessary to provide factual support for motion.

Authority:

Cal Rules Ct, Rule 3.1112(b)

Form:

See 11.21

- ☐ Prepare meet-and-confer declaration.

Authority:

CCP §§ 2016.040, 2031.060(a)

Discussion:

See 11.04

- ☐ Prepare proposed order.

Authority:

Cal Rules Ct, Rule 3.1112(b)

Form:

See 11.22

- ☐ Follow standard procedure for noticed motion.



Timing:

Motion should be made "promptly" [CCP § 2031.060(b)]

Authority:

Cal Rules Ct, Rule 3.1300 et seq.



Cross Reference:

Standard format for noticed motion, see *Matthew Bender Practice Guide: California Pre-Trial Civil Procedure*, Ch. 26, 26.39-26.45.



23 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 11 Seeking or Opposing Protective Order

II. SEEKING PROTECTIVE ORDER AGAINST DEMAND FOR ELECTRONICALLY STORED INFORMATION

*1-11 MB Practice Guide: CA E-Discovery and Evidence 11.04***11.04 Options and Strategies.**

On receiving a demand for the production of electronically stored information, the responding party may opt to move for a protective order, rather than respond with an objection and wait for a motion to compel a further response [see *CCP* §§ 2031.060(a), 2031.210, 2031.310]. As the moving party seeking a protective order, the responding party will have the first chance to frame the discovery issues.

Cross Reference:

Discussion of responding to demand for discovery of electronically stored information, see *Ch. 8, Responding to Electronic Discovery Requests in California*, 8.12-8.23.

Discussion of asserting objections to demand, see *Ch. 10, Opposing Demands for Production of Electronic Evidence in California Court*, 10.09-10.14.

Discussion of making and opposing motion to compel, see *Ch. 12, Obtaining or Opposing Motion to Compel*.

Timing:

A protective order must be sought promptly, but only after a good-faith attempt at informal resolution through a meeting and conference between counsel (sometimes called a "meet and confer") [*CCP* §§ 2016.040, 2031.060(a)]. A declaration of attempts to meet and confer must be filed with the motion [*CCP* § 2031.060(a)].

Cross Reference:

Discussion of meet-and-confer requirement, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management*, 5.14-5.25.

Warning:

Monetary sanctions may be imposed on the respondent for either unsuccessfully seeking a protective order, or for objecting and later losing a motion to compel [*CCP* §§ 2031.060(h) (protective order), 2031.300(c) (motion to compel)]. Due to the risk of sanctions, counsel for the responding party should attempt to resolve the issues informally. If informal resolution is not possible, counsel should develop an

argument and facts that the position taken in seeking a protective order was "substantially justified" in order to avoid sanctions.

➡ **Cross Reference:**

Discussion of sanctions, see 11.13-11.15; see also *Ch. 13, Seeking or Opposing Sanctions for Noncompliance*, 13.03-13.10.

Compare--Nonparty Subpoena:

The demanding party must take reasonable steps to avoid imposing an undue burden or expense on a nonparty who is subpoenaed to produce electronically stored information [*CCP* § 1985.8(j)]. Similarly, a court order compelling compliance with a subpoena for the production of electronically stored information must protect a person who is neither a party nor a party's officer from undue burden or expense see *CCP* § 1985.8(k)]. Thus, a subpoenaed person should oppose the subpoena if it imposes an undue burden or expense.

➡ **Cross Reference:**

Discussion of procedure for obtaining electronically stored information from nonparty, see *Ch. 6, Demanding Production of Electronically Stored Information in California Court*, 6.14-6.19.



24 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 11 Seeking or Opposing Protective Order

II. SEEKING PROTECTIVE ORDER AGAINST DEMAND FOR ELECTRONICALLY STORED INFORMATION

1-11 MB Practice Guide: CA E-Discovery and Evidence 11.05

11.05 Protective Order May Issue If Demanded Electronic Discovery Creates Undue Burden or Expense.

The party seeking a protective order regarding production, inspection, copying, testing, or sampling of electronically stored information may seek the order on one of four traditional bases [CCP § 2031.060(b); see also CCP § 2017.020(a)]:

- Unwarranted annoyance.
- Embarrassment.
- Oppression.
- Undue burden or expense.

Cross Reference:

Discussion of protective orders generally, see *Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 1, Strategy and Planning, 1.15*.

The most frequently urged basis for a protective order against a demand for electronically stored information is that the information is not reasonably accessible because of undue burden or expense [see CCP § 2031.060(b)-(f)].



Strategic Point--Reasonable Alternative:

Instead of immediately seeking a protective order, the responding party may assert an objection that the information is not reasonably accessible because of undue burden or expense and that the responding party will not search the source in the absence of an agreement with the demanding party or court order. The objection must identify the types or categories of sources of electronically stored information that are not reasonably accessible. If it is included in a timely response to the demand, such an objection will preserve any other objections the responding party may have to the information specified in the objection [CCP § 2031.210(d)].

Cross References:

Discussion of response to demand for production of electronically stored information, see *Ch. 8, Responding to Electronic Discovery Requests in California Court*, 8.12-8.23.

Discussion of asserting objection in response, see *Ch. 10, Opposing Demands for Production of Electronic Evidence in California Court*, 10.09-10.14.

Compare--Protective Order Sought by Subpoenaed Nonparty:

A nonparty who is subpoenaed to produce electronically stored information may move for a protective order on the ground that the information sought is not reasonably accessible because of undue burden or expense, or that the burden, expense, or intrusiveness of the demanded discovery outweighs the likelihood that the information sought will lead to the discovery of admissible evidence [*CCP* § 2017.020(a); see *CCP* § 1985.8(d)].



25 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 11 Seeking or Opposing Protective Order

II. SEEKING PROTECTIVE ORDER AGAINST DEMAND FOR ELECTRONICALLY STORED INFORMATION

1-11 MB Practice Guide: CA E-Discovery and Evidence 11.06

11.06 Responding Party Must Demonstrate That Source Is Not Reasonably Accessible.

11.06[1] Responding Party Has Burden of Persuasion. A responding party seeking a protective order on the ground that the electronically stored information is from a source that is not reasonably accessible because of undue burden or expense has the burden of demonstrating the existence of that circumstance [*CCP* § 2031.060(c); see *CCP* § 1985.8(d) (nonparty opposing subpoena for electronically stored information has similar burden of persuasion)].

Strategic Points:



- A declaration by an expert may be necessary to establish the burden and expense that would be associated with complying with the discovery demand.
- If possible, counsel for the responding party should show that alternative discovery would be sufficient for the needs of the demanding party or of the case. Even if the motion for a protective order is denied, alternative discovery options are grounds for the court to impose limits on the frequency or extent of discovery [*CCP* § 2031.060(f)(1), (2), (g)].



Cross References:

Discussion of court's power to impose limits on frequency or extent of discovery, see 11.19.

Discussion of court's power to shift costs to demanding party, see 11.12.

11.06[2] Source May Be Not Reasonably Accessible If Information Is Not Readily Usable. The governing statute provides for the issuance of a protective order if the information sought is "from a source that is not reasonably accessible because of undue burden or expense" [*CCP* § 2031.060(c)-(e); compare *Fed R Civ P* 26(b)(2)(B) (party need not provide discovery of electronically stored information from sources that are "not reasonably accessible because of undue burden or cost")]. Although there are no bright line rules for courts to follow, the "burden and expense" referred to often involves putting the demanded information into a usable form. Thus, information may be considered

"accessible" if it is stored in a readily usable format and does not need to be restored or otherwise manipulated to be usable. "Inaccessible" data, on the other hand, may not be readily usable [see *Zubulake v. UBS Warburg LLC* (SDNY 2003) 217 FRD 309, 318-320 ("[w]hether electronic data is accessible or inaccessible turns largely on the media on which it is stored")].

Examples:

Examples of "accessible" sources likely include computer hard drives, optical disks, and offline storage or archives that use magnetic tapes or optical disks. For such sources, the time it takes to actually access the data can range from milliseconds to days, but the data is considered accessible because it does not need to be restored or otherwise manipulated to be usable. In contrast, backup tapes or erased, fragmented, or damaged data are not considered accessible: backup tapes must be restored, fragmented data must be defragmented, and erased data must be reconstructed before it can be used [see *Zubulake v. UBS Warburg LLC* (SDNY 2003) 217 FRD 309, 318-320] .

In addition to the factor of the file access time, additional factors that courts may consider in accessibility determinations include the volume of information to be searched, how likely it is to include relevant information, whether the data will likely duplicate other sources of information.

Consider--Statutory Language:

The statute governing protective orders refers both to "undue burden *and* expense" [CCP § 2031.060(b) (emphasis added)] and to "undue burden *or* expense" [CCP § 2031.060(c), (d) (emphasis added)]. The difference in language could be attributed to a drafting oversight (the "and" provision and the "or" provisions were enacted at different times). If the use of different terms was deliberate, it is unclear what meanings were intended. As a practical matter, it is difficult to imagine an undue burden that would not be associated with excessive or undue expense.

11.06[3] Court May for Good Cause Order Discovery of Inaccessible Information. If the responding party establishes that the electronically stored information is from a source that is not reasonably accessible, the court may nonetheless order discovery if the demanding party shows good cause [CCP § 2031.060(d); see CCP § 1985.8(e) (similar provision applicable when nonparty establishes that subpoenaed electronically stored information is not reasonably accessible)]. In such a case, the court may limit the frequency or extent of discovery [see CCP § 2031.060(f); see also CCP § 1985.8(h)].

 Cross Reference:

Discussion of good cause for discovery of inaccessible information, see 11.11.



26 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 11 Seeking or Opposing Protective Order

II. SEEKING PROTECTIVE ORDER AGAINST DEMAND FOR ELECTRONICALLY STORED INFORMATION

1-11 MB Practice Guide: CA E-Discovery and Evidence 11.07

11.07 Court Has Broad Power to Make Protective Orders.

11.07[1] Protective Orders Are Designed To Prevent Discovery Abuses. Protective orders are meant to prevent unwarranted annoyance, embarrassment, oppression, or undue burden and expense [*CCP § 2031.060(b)*]. The court has broad powers to issue protective orders: it may craft "any order that justice requires" to protect the parties from these discovery abuses [*CCP § 2031.060(b)*].

11.07[2] Protective Order Need Not Deny Demanded Discovery. A protective order need not deny discovery of the electronically stored information sought. The order may allow discovery but reduce or mitigate the production challenges faced by the responding party, by directing the parties to take different actions than those originally specified in the discovery demand [*see CCP § 2031.060(b)*].

Examples:

A protective order may include, but is not limited to, any of the following directions [*CCP § 2031.060(b)*]:

- That all or some of the information demanded need not be produced or made available at all.
- That the time for a response to a set of demands, or to a particular item or category in the set of demands be extended.
- That the place of production be other than that specified in the demand.
- That the inspection, copying, testing, or sampling be made only on specified terms and conditions.
- That a trade secret or other confidential research, development, or commercial information not be disclosed, or be disclosed only to specified persons or only in a specified way.
- That the items produced be sealed and thereafter opened only on order of the court.

➡ Cross Reference:

Discussion of court's power to limit frequency and extent of discovery of electronically stored information, see *Ch. 10, Opposing Demands for Production of Electronic Evidence in California Court*, 10.12[5].



27 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 11 Seeking or Opposing Protective Order
III. OPPOSING MOTION FOR PROTECTIVE ORDER

1-11 MB Practice Guide: CA E-Discovery and Evidence 11.08

11.08 CHECKLIST: Opposing Motion for Protective Order.

☐ Prepare papers opposing motion for protective order.

☐ Prepare memorandum opposing motion, including following as appropriate:

Authority:

Cal Rules Ct, Rules 3.1112(a)(3), 3.1113

☐ Argument that demanded electronically stored information is reasonably accessible.

Authority:

CCP § 2031.060(c)

Discussion:

See 11.10

☐ Argument that, even if demanded electronically stored information is not reasonably accessible, good cause for discovery exists.

Authority:

CCP § 2031.060(d)

Discussion:

See 11.11

☐ Suggestion of conditions, such as sharing of discovery costs, that court might impose to lessen burden or expense

of discovery.

Authority:

CCP § 2031.060(e)

Discussion:

See 11.12

☐ Request for monetary sanction.

Authority:

CCP § 2031.060(h)

Discussion:

See 11.15

☐ Prepare affidavits or declarations, including expert declarations, along with any appropriate exhibits, that are necessary to provide factual support for opposition.

Authority:

Cal Rules Ct, Rule 3.1112(b)

☐ Follow standard procedure for opposing noticed motion.

Authority:

Cal Rules Ct, Rule 3.1300 et seq.

Discussion:

See *Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure, Ch. 26, 26.39-26.45.*



28 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 11 Seeking or Opposing Protective Order
III. OPPOSING MOTION FOR PROTECTIVE ORDER

1-11 MB Practice Guide: CA E-Discovery and Evidence 11.09

11.09 Options and Strategies.

When faced with a motion for a protective order based on a claim that electronically stored information sought is from a source that is not reasonably accessible, the demanding party may oppose the motion by demonstrating that the source is reasonably accessible [*see CCP § 2031.060(c)*].

➡ **Cross Reference:**

Discussion of showing that information sought is reasonably accessible, see *11.10*.

If the court finds that the electronically stored information sought is not reasonably accessible, the demanding party may nevertheless obtain discovery by showing that there is good cause for discovery [*CCP § 2031.060(d)*].

➡ **Cross References:**

Discussion of good cause for discovery of information that is not reasonably accessible, see *11.11*.

Discussion of court's power to set conditions for discovery after finding good cause for discovery, see *11.12*.



29 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 11 Seeking or Opposing Protective Order
III. OPPOSING MOTION FOR PROTECTIVE ORDER

1-11 MB Practice Guide: CA E-Discovery and Evidence 11.10

11.10 Demanding Party May Demonstrate That Electronic Information Is Reasonably Accessible.

If a motion for a protective order is based on a claim that the electronically stored information sought is from a source that is not reasonably accessible, the demanding party may oppose the motion by demonstrating that the source is reasonably accessible [*see CCP § 2031.060(c)*]. This requires a showing that obtaining the demanded information from the source will not entail undue burden or expense [*see CCP § 2031.060(c)*].

Whether electronic data is accessible or inaccessible depends largely on the media on which it is stored; even if it would take days to retrieve a particular storage medium, the stored information may be deemed accessible if it does not need to be restored or otherwise manipulated to be usable [*see Zubulake v. UBS Warburg LLC (SDNY 2003) 217 FRD 309, 318-320*].

➤ **Cross Reference:**

Discussion and examples of accessible and inaccessible sources of electronically stored information, see *11.06[2]*.

Consider:

Even if the court finds that the source of the information is reasonably accessible, the court must limit the frequency or extent of discovery if certain conditions exist [*CCP § 2031.060(f)*].

➤ **Cross Reference:**

Discussion of orders limiting frequency or extent of discovery, see *11.19*.



30 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 11 Seeking or Opposing Protective Order
III. OPPOSING MOTION FOR PROTECTIVE ORDER

1-11 MB Practice Guide: CA E-Discovery and Evidence 11.11

11.11 Demanding Party May Obtain Discovery of Information That Is Not Reasonably Accessible by Demonstrating Good Cause.

11.11[1] Showing of Good Cause May Overcome Finding That Information Is Not Reasonably Accessible. If the court finds the source of the electronically stored information is not reasonably accessible because of undue burden or expense, the court may nonetheless order discovery if the demanding party shows good cause [*CCP § 2031.060(d)*; *see CCP § 1985.8(e)* (similar provision applicable when nonparty establishes that subpoenaed electronically stored information is not reasonably accessible)].

Consider:

Even if the court finds that there is good cause for discovery, the court may set conditions for the discovery, including the allocation of the expense of discovery [*CCP § 2031.060(e)*; *see CCP § 1985.8(f)* (applicable when nonparty opposes subpoena for electronically stored information)]. Moreover, under certain circumstances the court must limit the frequency or extent of discovery [*CCP § 2031.060(d), (f)*; *see CCP § 1985.8(e), (h)* (applicable when nonparty opposes subpoena for electronically stored information)].

➡ **Cross References:**

Discussion of court-imposed conditions for discovery and allocation of expense, *see 11.12*. Discussion of circumstances that require court to limit frequency or extent of discovery, *see 11.19[2]-[5]*.

11.11[2] Court May Consider Several Factors in Determining Good Cause. Although the statute is silent on what constitutes "good cause," factors relevant to the court's determination of good cause may include the following [*CCP § 2031.060(f)* (findings that will result in order limiting discovery even of reasonably accessible data); *see CCP § 1985.8(h)* (applicable when nonparty opposes subpoena for electronically stored information)]:

- Whether it is possible to obtain the demanded information from some other source that is more convenient, less burdensome, or less expensive.
- Whether the discovery sought is unreasonably cumulative or duplicative.

- Whether the demanding party has had ample opportunity for discovery in the action to obtain the information sought.
- Whether the likely burden or expense outweighs the likely benefit, considering the amount in controversy, resources of the parties, importance of the issues and importance of the demanded information in resolving the issues.

Compare--Similar Factors Under Federal Rule:

The Federal Rules of Civil Procedure are substantially similar to California's Civil Discovery Act in allowing discovery of electronically stored information from a source that is not reasonably accessible if the demanding party shows good cause [*compare Fed R Civ P 26(b)(2)(B) with CCP § 2031.060(d)*]. Under the federal rules, the determination of good cause to require a party to search for and produce electronically stored information from a source that is not reasonably accessible depends not only on the burdens and costs of doing so, but also on whether those burdens and costs can be justified in the circumstances of the case. Appropriate considerations may include the following [*see Committee Note of 2006 to Fed R Civ P 26(b)(2)*]:

- The specificity of the discovery demand.
- 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.
- The parties' resources.

Strategic Point--Demanding Party:



To demonstrate good cause for discovery despite undue burden and expense, the demanding party should be prepared to do the following:

- Show the need for the demanded discovery in light of the issues in the case and the alternatives for discovery.
- Show, using expert testimony if necessary, that any inconvenience to the responding party will be justified, and that the chances of harm to the responding party will be minimized [*see Playboy Enters. v. Welles (SD Cal 1999) 60 F Supp2d 1050, 1054-1055*].
- Show a history of good faith meet-and-confer attempts to resolve the issue.

Example:

If the responding party claims that compliance with the discovery demand would cause a disruption of the responding party's business, counsel for the demanding party should offer, at the meet-and-confer and in opposing the motion, to schedule the demanded discovery at a time that would minimize the disruption to the responding party's business [see *Playboy Enters. v. Welles* (SD Cal 1999) 60 F Supp2d 1050, 1054-1055] .

11.11[3] Court May Order Sampling or Testing to Aid in Determining Existence of Good Cause for Discovery. If it is not precisely known what information is contained in an inaccessible source, limited discovery--"sampling" or testing--may be helpful in determining whether there is good cause for full production of the demanded information [see CCP § 2031.010(e)]. In an appropriate case, sampling can help the parties and the court assess the likely benefits and probable cost of full discovery [see *Hill v. Eddie Bauer* (CD Cal 2007) 242 FRD 556, 564 (allowing sampling, because full response to demand would have been unduly burdensome); *Toshiba America Electronics Components v. Superior Court* (2004) 124 CA4th 762, 21 CR3d 532 (encouraging parties to meet and confer regarding sampling of backup tapes)].



31 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 11 Seeking or Opposing Protective Order
III. OPPOSING MOTION FOR PROTECTIVE ORDER

1-11 MB Practice Guide: CA E-Discovery and Evidence 11.12

11.12 Court May Set Conditions for Discovery After Finding Good Cause.

11.12[1] Court May Set Conditions and Allocate Discovery Expenses. If the court finds good cause for the production of electronically stored information from a source that is not reasonably accessible, the court may allocate the expense of discovery and set other discovery conditions [*CCP* § 2031.060(e); see *CCP* § 1985.8(f) (applicable when nonparty opposes subpoena for electronically stored information)].



Strategic Point:

To lessen the burden of discovery, counsel may suggest to the court such conditions as sampling or testing of a given source of electronically stored information, rather than full production [see *Hill v. Eddie Bauer (CD Cal 2007) 242 FRD 556, 564* (allowing sampling, because full response to demand would have been unduly burdensome)]; scheduling production of demanded information in stages; or requiring production in a format that is less expensive than the format specified in the discovery demand.

11.12[2] Demanding Party Must Pay Cost of Translating Data Compilations. If translation of any data compilations included in the demand is necessary to put the demanded information in a reasonably usable form, the responding party, using "detection devices," must translate the information, and the demanding party must pay the reasonable expense of that translation [*CCP* § 2031.280(e); *Toshiba Am. Elec. Components, Inc. v. Superior Court (2004) 124 CA4th 762, 769-772, 21 CR3d 532* (cost shifting under substantially identical predecessor of *CCP* § 2031.280(e) is mandatory); see also *CCP* § 1985.8(g) (similar requirement when nonparty is subpoenaed to produce electronically stored information)].



Strategic Point:

The imposition of the cost of translating data compilations on the demanding party is mandatory [*CCP* §§ 1985.8(g), 2031.280(e)]. However, the governing statutes do not define the terms "detection devices" and "translate." In one case, the parties did not dispute that backup tapes were "data compilations" and that manipulation of the tapes to produce usable information constituted translation of the data [see *Toshiba Am. Elec. Components, Inc. v. Superior Court (2004) 124 CA4th 762, 767, 21 CR3d 532*].

However, if there is any question whether the production of electronically stored information in a given case involves the use of "detection devices" to "translate" a data compilation, the parties may offer expert evidence in an attempt to convince the court that the production does (or does not) fall within the scope of these cost-shifting provisions. In addition, because only "reasonable" expenses of translation are to be paid by the demanding party, the determination of what cost is reasonable is a matter for the discretion of the court and on which the parties may offer evidence and argument [*Toshiba Am. Elec. Components, Inc. v. Superior Court* (2004) 124 CA4th 762, 773, 21 CR3d 532] .



Cross Reference:

Discussion of cost shifting when production of demanded information requires translation of data compilations, see *Ch. 9, Gathering and Producing Electronically Stored Information*, 9.10, 9.35.

11.12[3] Court May Shift Significant or Special Costs When Inaccessible Information Is Sought. Aside from the mandatory shifting of the cost of translating data compilations [see *CCP §§ 1985.8(g), 2031.280(e)*], a court generally has discretion to shift costs to the demanding party when the production of information that is not reasonably accessible generates significant or special costs [see *Zubulake v. UBS Warburg LLC* (SDNY 2003) 216 FRD 280, 284 ("[i]t is worth emphasizing again that cost-shifting is potentially appropriate only when *inaccessible* data is sought. When a discovery request seeks accessible data--for example, active on-line or near-line data--it is typically inappropriate to consider cost-shifting")].

In determining whether to shift costs for producing relatively inaccessible data, the court may consider the following factors [see *OpenTV v. Liberate Techs.* (ND Cal 2003) 219 FRD 474, 476-477 ; *Zubulake v. UBS Warburg LLC* (SDNY 2003) 216 FRD 280, 284] :

- The extent to which the demand is specifically tailored to discover relevant information.
- The availability of the information from other sources.
- The total cost of production, compared with the amount in controversy.
- The total cost of production, compared with 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.
- The relative benefits to the parties of obtaining the information.

Consider:

When the court finds good cause to order production, it has already found that the responding party (i.e., the party moving for a protective order) carries an undue burden or expense, but that discovery must nevertheless proceed [see *CCP § 2031.060(d)*]. Consequently, the court may be receptive to setting conditions or allocating discovery expenses to reduce the burden or expense borne by the responding party. Thus, the responding party should demonstrate any anticipated hardship in complying with discovery demands and propose reapportionment of expenses or new conditions of discovery that will reduce unfairness.

Example:

A responding party argued that by agreeing to make its complete database available for inspection and copying, it had satisfied its obligations by making the source code available for inspection in the order

and manner in which it was kept in the ordinary course of business [see *CCP § 2031.280(a)*]. The court found that it would take between 125 and 150 hours of work to complete the extraction process for the multiple versions of source code sought by the demanding party and that the demanded electronic data was stored in a format that was not reasonably accessible. Since the demanded source code was highly likely to contain relevant information and was unavailable from another source, the court found cost-shifting appropriate. Because the parties were similarly situated (both were corporations), the court ordered the parties to split equally the cost of extracting the source code, with the responding party to bear the cost of making the demanded copy [*OpenTV v. Liberate Techs. (ND Cal 2003) 219 FRD 474, 476-479*] .

**Cross References:**

Discussion of mandatory shifting of cost of translating data compilations, see *11.12[2]*. Discussion of potential for cost-shifting as consideration in planning discovery, see *Ch. 4, Planning E-Discovery, 4.18*. Discussion of ethical issues involved in running up discovery costs, see *Ch. 3, Ethical Issues for Attorneys in E-Discovery, 3.10*.



32 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 11 Seeking or Opposing Protective Order

IV. AVOIDING MONETARY SANCTIONS FOR SEEKING OR OPPOSING PROTECTIVE ORDER

1-11 MB Practice Guide: CA E-Discovery and Evidence 11.13

11.13 CHECKLIST: Avoiding Monetary Sanctions for Seeking or Opposing Protective Order.

- ☐ Before motion for protective order is made, engage in good-faith effort to resolve dispute informally, by meeting and conferring with opposing counsel.

Authority:

CCP §§ 2016.040, 2031.060(a)

Discussion:

See 11.14, 11.15[1]

- ☐ Be prepared to propose or accept reasonable compromise of client's position in order to facilitate reasonably cost-effective discovery.
- ☐ Carefully document informal efforts to resolve dispute at meet-and-confer, and describe those efforts in declaration accompanying moving or opposing papers if motion is filed.
- ☐ If court rules against client on motion for protective order, demonstrate any of following:
- ☐ That client acted with substantial justification.

Authority:

CCP § 2031.060(h)

Discussion:

See 11.15[1]

- ☐ That other circumstances make imposition of sanctions on client unjust.

Authority:

CCP § 2031.060(h)

Discussion:

See 11.15[2]

- ☐ If client's motion for protective order was denied, that demanded information was lost, damaged, altered, or overwritten as result of routine, good-faith operation of electronic information system.

Authority:

CCP § 2031.060(i)(1)

Discussion:

See 11.15[3]



33 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 11 Seeking or Opposing Protective Order

IV. AVOIDING MONETARY SANCTIONS FOR SEEKING OR OPPOSING PROTECTIVE ORDER

1-11 MB Practice Guide: CA E-Discovery and Evidence 11.14

11.14 Options and Strategies.

Parties are encouraged to resolve discovery disputes outside of the judicial process because court supervision often comes at a price [see *CCP* § 2031.060(a) (motion for protective order must be accompanied by meet-and-confer declaration under *CCP* § 2016.040)]. In most cases, the court must impose monetary sanctions on the losing party on a motion for a protective order, thereby exacting a penalty for use of the court's resources to resolve a discovery dispute [*CCP* § 2031.060(h); see also *CCP* § 2023.030(a) (if money sanction is authorized by any provision of Civil Discovery Act, court ordinarily must impose that sanction)].

► Cross Reference:

Discussion of seeking or opposing sanctions for noncompliance with demand for discovery of electronically stored information, see *Ch. 13, Seeking or Opposing Sanctions for Noncompliance, 13.11-13.15*.

A party that unsuccessfully makes or opposes a motion for a protective order may avoid sanctions, however, by demonstrating that the party acted with substantial justification in refusing to produce or in demanding production of the electronically stored information, or that other circumstances make the imposition of sanctions unjust [*CCP* § 2031.060(h)].

► Cross References:

Discussion of substantial justification for party's conduct, see *11.15[1]*.

Discussion of other circumstances making imposition of sanctions unjust, see *11.15[2]*.

In addition, the party that moved for a protective order may avoid sanctions for failing to produce electronically stored information by showing that the information was lost due to routine, good-faith operation of an electronic information system, and that there are no exceptional circumstances justifying sanctions [*CCP* § 2031.060(i)(1)].

► Cross Reference:

Discussion of good-faith loss of electronically stored information, see *11.15[3]*.



34 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 11 Seeking or Opposing Protective Order

IV. AVOIDING MONETARY SANCTIONS FOR SEEKING OR OPPOSING PROTECTIVE ORDER

1-11 MB Practice Guide: CA E-Discovery and Evidence 11.15

11.15 Losing Party May Avoid Monetary Sanctions.

11.15[1] Losing Party May Avoid Sanctions by Showing Substantial Justification for Losing Position.

Although sanctions generally must be imposed on the losing party on a motion for a protective order [*CCP* § 2031.060(h); *see also CCP* § 2023.030(a)], monetary sanctions will not be imposed if the losing party shows that it acted with substantial justification [*CCP* § 2031.060(h); *see also CCP* § 2023.030(a) (money sanction authorized by any provision of Civil Discovery Act need not be imposed if court finds that party acted with substantial justification)].



Strategic Point:

To establish substantial justification for a position that the court ultimately rejected, a party should show that, before the motion was decided, the application of established statutory and case law to the facts was unclear, so that a ruling from the court was required to resolve a legitimate dispute.



Cross Reference:

Discussion of avoiding sanctions by showing other circumstances make sanctions unjust, *see 11.15[2]*.

11.15[2] Losing Party May Avoid Sanctions by Showing That Imposition of Sanctions Would Be Unjust.

Although sanctions generally must be imposed on the losing party on a motion for a protective order [*CCP* § 2031.060(h); *see also CCP* § 2023.030(a)], monetary sanctions will not be imposed if the losing party shows that circumstances make the imposition of the sanction unjust [*CCP* § 2031.060(h)]. This exception to imposition of discovery sanctions applies when the losing party cannot provide a substantial justification for its actions, but the sanctions are otherwise unjust under a separate set of considerations [*see CCP* § 2031.060(h)].



Cross Reference:

Discussion of avoiding sanctions by showing that party's position was substantially justified, *see 11.15[1]*.

11.15[3] Losing Party May Avoid Sanctions by Showing That Information Was Lost in Good Faith. The court may not impose sanctions on a party that unsuccessfully moves for a protective order, absent exceptional circumstances, if the responding party cannot produce the demanded discovery because the electronically stored information was lost,

damaged, altered, or overwritten as the result of the routine, good-faith operation of an electronic information system [CCP § 2031.060(i)(1); see CCP § 1985.8(l)(1) (applicable when nonparty is subpoenaed to produce electronically stored information)].



35 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 11 Seeking or Opposing Protective Order

V. OBTAINING ALTERNATIVE RELIEF WHEN MOTION FOR PROTECTIVE ORDER IS DENIED

1-11 MB Practice Guide: CA E-Discovery and Evidence 11.16

11.16 CHECKLIST: Obtaining Alternative Relief When Motion for Protective Order Is Denied.

☐ If court denies motion for protective order based on finding of good cause for discovery:

Authority:

CCP § 2031.060(e), (g)

Discussion:

See 11.12, 11.18

☐ Remind court of evidence, including expert declarations, showing that demanded information is not reasonably accessible because of undue burden and expense.

☐ Make request, either in moving papers or at hearing on motion, that court to exercise its discretion to set terms and conditions for production of demanded information, including shifting all or part of cost of discovery to demanding party.

☐ Whether or not court found that demanded information is reasonably accessible, request (either as alternative in moving papers, or orally at hearing) that court limit frequency or extent of discovery of electronically stored information, based on evidence showing any of following:

Authority:

CCP § 2031.060(f)

Discussion:

See 11.19[1]

☐ It is possible to obtain demanded information from some other source that is more

convenient, less burdensome, or less expensive.

Discussion:

11.19[2]

- ☐ Discovery sought is unreasonably cumulative or duplicative.

Discussion:

11.19[3]

- ☐ Demanding party has had ample opportunity by discovery in action to obtain information sought.

Discussion:

11.19[4]

- ☐ Likely burden or expense of proposed discovery outweighs likely benefit, taking into account amount in controversy, resources of parties, importance of issues in litigation, and importance of demanded discovery in resolving those issues.

Discussion:

See *11.19[5]*



36 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 11 Seeking or Opposing Protective Order

V. OBTAINING ALTERNATIVE RELIEF WHEN MOTION FOR PROTECTIVE ORDER IS DENIED

1-11 MB Practice Guide: CA E-Discovery and Evidence 11.17

11.17 Options and Strategies.

If the court denies a motion for a protective order--for example, because the information sought is reasonably accessible, or because there is good cause for discovery of information that is not reasonably accessible--the court nevertheless may provide some relief by setting conditions for discovery (including allocation of expenses) or limiting the frequency or extent of discovery [*see CCP § 2031.060(d)-(f)*].

Consider:

Protective orders are often sought for the purpose of preventing excessive discovery costs. Even if the court denies the motion for a protective order, the court may provide other relief as necessary to mitigate the responding party's discovery costs. Therefore, counsel for the moving party should consider requesting other, alternative relief if the motion for a protective order is denied.

Cross References:

Discussion of court's power to set conditions for discovery, see *11.18*.

Discussion of court's power to limit frequency or extent of discovery, see *11.19*.



37 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 11 Seeking or Opposing Protective Order

V. OBTAINING ALTERNATIVE RELIEF WHEN MOTION FOR PROTECTIVE ORDER IS DENIED

1-11 MB Practice Guide: CA E-Discovery and Evidence 11.18

11.18 Court Has Discretion to Set Just Terms and Conditions for Discovery, Including Allocation of Expenses.

Even if the court denies a protective order, the moving party may obtain some relief through court-ordered changes in the conditions of discovery. Thus, if the court finds good cause for the production of electronically stored information that is not reasonably accessible, the court is authorized to set conditions for discovery of the information, including allocation of the expense of discovery [*CCP* § 2031.060(e); see *CCP* § 1985.8(f) (applicable when nonparty opposes subpoena for electronically stored information)]. Under a related provision, if the court denies the responding party's motion for a protective order, in whole or in part, the court may order the responding party to provide discovery "on terms and conditions that are just" [*CCP* § 2031.060(g)].

► Cross Reference:

Discussion of factors considered in determining whether to shift cost of producing information that is not reasonably accessible, see 11.12[3].

Compare--Discovery From Nonparty:

If the court's order requires compliance with a subpoena, the order must protect a person who is neither a party nor a party's officer from undue burden or expense resulting from compliance [*CCP* § 1985.8(k)].

Distinguish:

Under some circumstances, the court is required to limit the frequency or extent of discovery of electronically stored information [*CCP* § 2031.060(f); see *CCP* § 1985.8(h) (applicable when nonparty opposes subpoena for electronically stored information)].

► Cross Reference:

Orders limiting frequency or extent of discovery of electronically stored information, see 11.19.



38 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 11 Seeking or Opposing Protective Order

V. OBTAINING ALTERNATIVE RELIEF WHEN MOTION FOR PROTECTIVE ORDER IS DENIED

1-11 MB Practice Guide: CA E-Discovery and Evidence 11.19

11.19 Court Must Limit Frequency or Extent of Discovery of Electronically Stored Information Under Some Circumstances.

11.19[1] Limiting Order May Be Required Even If Protective Order Is Denied. Even if the court denies a motion for a protective order, it must limit the frequency or extent of discovery if it determines that any of four conditions specified by statute (discussed in 11.19[2] through 11.19[5], respectively) exists [*CCP* § 2031.060(f); see *CCP* § 1985.8(h) (applicable when nonparty opposes subpoena for electronically stored information)]. This requirement applies even if the court finds that the source of the information is reasonably accessible or that there is good cause for discovery of information that is not reasonably accessible [*CCP* § 2031.060(d), (f); see *CCP* § 1985.8(e), (h) (applicable when nonparty is subpoenaed to produce electronically stored information)].

Strategic Point:



Although the court could enter a limiting order sua sponte, it is advisable for the responding party to petition the court for intervention and to provide factual information that will allow the court to make the required findings.

Compare:

The federal rules also contain a provision authorizing a court to limit the frequency or extent of discovery of electronically stored information under the same circumstances described in the California statute [*compare Fed R Civ P 26(b)(2)(C) with CCP* § 2031.060(f)].



Cross References:

Discussion of circumstances that require court to limit frequency or extent of discovery, see 11.19[2]-[5].

Discussion of when information is not reasonably accessible, see 11.06[2].

Discussion of good cause for discovery, see 11.11.

Discussion of orders limiting frequency or extent of discovery under federal rules, see *Matthew*

Bender(R) Practice Guide: Federal Pretrial Civil Procedure in California, Ch. 22, 22.36-22.46.

11.19[2] Responding Party May Obtain Limiting Order by Showing Information Is Available From More Convenient Source. The court must limit the frequency or extent of discovery of electronically stored information, even when a protective order is not warranted, if it determines that it is possible to obtain the information from some other source that is more convenient, less burdensome, or less expensive [CCP § 2031.060(f)(1); see CCP § 1985.8(h)(1) (applicable when nonparty is subpoenaed to produce electronically stored information)].



Strategic Point:

Counsel for the responding party should compare the responding party's source of electronically stored information with other sources, in order to suggest to the court a more convenient, less burdensome, or less expensive source of discovery.

Example:

Generally, a court will not require production of electronically stored information from a source that is not "reasonably accessible" if the information is available from a more easily accessible source [see *Baker v. Gerould* (WDNY 2008) 2008 US Dist LEXIS 28628, at *6-*7]. Thus, for example, the court may decide that a party need not produce e-mails from backup tapes or PDAs/Blackberries/iPhones if production from another source (such as a corporate e-mail server) is available and is likely to include all or most of the data that would be on the other sources.

11.19[3] Responding Party May Obtain Limiting Order by Showing Discovery Sought Is Unreasonably Cumulative or Duplicative. The court must limit the frequency or extent of discovery of electronically stored information, even when a protective order is not warranted, if it determines that the discovery sought is unreasonably cumulative or duplicative [CCP § 2031.060(f)(2); see CCP § 1985.8(h)(2) (applicable when nonparty is subpoenaed to produce electronically stored information)].



Strategic Point:

The court may not be aware that the discovery sought is cumulative or duplicative, either in the current demand, or as compared with previous discovery. Therefore, counsel for the responding party should review the current discovery demand, as well as other discovery provided or demanded by any party, and bring any unreasonably cumulative or duplicative aspect of the current demand to the court's attention.

Distinguish:

A discovery demand that minimally overlaps other discovery does not trigger the court's duty to limit the frequency or extent of discovery of electronically stored information. Rather, to obtain a limiting order, the responding party must demonstrate that the demanded discovery is *unreasonably* cumulative or duplicative [CCP § 2031.060(f)(2); see CCP § 1985.8(h)(2) (applicable when nonparty is subpoenaed to produce electronically stored information)]. Thus, the responding party should do the following:

- Establish that the discovery sought contains extensive, rather than incidental, duplication and accumulation of information.
- Explain why the duplication or accumulation is an unnecessary waste of resources.

Example--Discovery Not Unreasonably Cumulative:

It is not unreasonably duplicative for a party to seek additional evidence on the same disputed issue for

which it already possesses probative evidence [*City of King City v. Community Bank of Cent. Cal.* (2005) 131 CA4th 913, 933, 32 CR3d 384] .

Consider--Importance of Issue:

Whether a discovery demand is *unreasonably* cumulative may depend in part on the importance of the issue at stake [see *OpenTV v. Liberate Techs.* (ND Cal 2003) 219 FRD 474, 476-477 (listing importance of issue as factor in deciding whether to shift costs of discovery)]. If it is a minor issue, and it can be proven or refuted with other more readily available evidence, the court might be more likely to find that the discovery demand is unreasonably cumulative.

11.19[4] Responding Party May Obtain Alternative Relief by Showing That Demanding Party Wasted Previous Opportunity for Discovery. The court must limit the frequency or extent of discovery of electronically stored information, even when a protective order is not warranted, if it determines that the demanding party has had ample opportunity by discovery in the action to obtain the information sought [CCP § 2031.060(f)(3); see CCP § 1985.8(h)(3) (applicable when nonparty is subpoenaed to produce electronically stored information)]. Stated another way, when the demanding party has failed to utilize other discovery opportunities (including other opportunities for discovery of electronically stored information) to obtain the demanded information, the court must limit the scope of the electronic discovery available.



Strategic Point--Responding Party:

The court may not be aware of other opportunities for discovery that the demanding party failed to take advantage of. Therefore, counsel for the responding party should provide the court with details of previous discovery opportunities or other available sources that the demanding party failed to utilize.



Strategic Point--Demanding Party:

This provision requires a disciplined approach to discovery of electronically stored information [see CCP § 2031.060(f)(3); see also CCP § 1985.8(h)(3) (applicable when nonparty is subpoenaed to produce electronically stored information)]. If a party delays document review until the approach of trial, the court may decide that the party has wasted its opportunity for discovery of important information and that discovery of electronically stored information should not be permitted.

11.19[5] Responding Party May Obtain Alternative Relief by Showing That Burden or Expense of Discovery Outweighs Benefit. The court must limit the frequency or extent of discovery of electronically stored information, even when a protective order is not warranted, if it determines that the likely burden or expense of the proposed discovery outweighs the likely benefit, considering the amount in controversy, the resources of the parties, the importance of the issues in the litigation, and the importance of the demanded discovery in resolving the issues [CCP § 2031.060(f)(4); see CCP § 1985.8(h)(4) (applicable when nonparty is subpoenaed to produce electronically stored information)].

Consider:

This is a catch-all provision that may allow counsel for the responding party to inform the court of the real evidentiary issues in the case, and to argue for limits on demands for discovery of electronically stored information that go beyond what is really in dispute. Arguments that counsel might make include the following [see CCP § 2031.060(f)(4)]:

- The burden or expense that the responding party must undergo to provide the demanded discovery outweighs the amount in controversy or any benefit to be gained by the demanding party.

- The responding party possesses so few or limited resources, in comparison with those of the demanding party, that the discovery should be limited.
- The issues underlying the discovery demand are not significant enough to warrant the burden or expense of the producing the information sought.
- The demanded discovery will not have an appreciable impact on resolving the issues in the case and therefore is not justified.



39 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 11 Seeking or Opposing Protective Order
VI. FORMS

*1-11 MB Practice Guide: CA E-Discovery and Evidence 11.20***11.20 Notice of Motion and Motion for Protective Order.**

Notice of Motion and Motion for Protective Order.

Tom Doe

California Bar Number 987654

100 North Main St., Suite 200

Farallon City, California 90000

Phone: 555-555-5555

Attorney for Plaintiff, John Smith

SUPERIOR COURT OF CALIFORNIA,

COUNTY OF FARALLON

John Smith, Plaintiff, vs. Mary Jones Enterprises,
Inc., Defendant.

)
) No. _____
) NOTICE OF MOTION AND MOTION
) FOR PROTECTIVE ORDER
) Date: _____
) Time: _____
) Location: _____
) Judge: _____
) Date Action Filed: _____
) Trial Date: _____
)

To Defendant, Mary Jones Enterprises, Inc., and its attorney of record:

NOTICE IS HEREBY GIVEN that, on _____ [date], at _____ [time], or as soon
thereafter as the matter may be heard, in [_____ (Department or Division) _____ of]
this court, located at 1 North Main Street, Farallon City, California, Plaintiff, John Smith, will, and hereby does, move
for an order providing that Plaintiff need not respond to Demand No. 3 of Defendant's First Set of Demands for
Production of Electronically Stored Information, and awarding sanctions against Defendant.

The motion is based on this notice of motion, the accompanying declaration(s) of _____ [*name(s)*], the meet-and-confer declaration of the undersigned, the accompanying supporting memorandum, the records and file herein, and such evidence as may be presented at the hearing on the motion.

Dated: _____

Respectfully submitted,

_____ [*signature*]

Tom Doe

Attorney for Plaintiff, John Smith

NOTES:

Authority:

CCP § 2031.060

Checklist:

See 11.03

Discussion:

See 11.04, 11.05

Related Form for Declaration Supporting Motion:

See 11.21

Related Form for Order:

See 11.22



40 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 11 Seeking or Opposing Protective Order
VI. FORMS

1-11 MB Practice Guide: CA E-Discovery and Evidence 11.21

11.21 Declaration Supporting Motion for Protective Order.

Declaration Supporting Motion for Protective Order.

Tom Doe

California Bar Number 987654

100 North Main St., Suite 200

Farallon City, California 90000

Phone: 555-555-5555

Attorney for Plaintiff, John Smith

SUPERIOR COURT OF CALIFORNIA,

COUNTY OF FARALLON

John Smith, Plaintiff, vs. Mary Jones Enterprises,
Inc., Defendant.

)
) No. _____
) DECLARATION OF _____ [e.g.,
) JOHN SMITH] IN SUPPORT OF
) MOTION FOR
) PROTECTIVE ORDER
) Date: _____
) Time: _____
) Location: _____
) Judge: _____
) Date Action Filed: _____
) Trial Date: _____

I, _____ [e.g., John Smith], declare:

1. I am _____ [e.g., the Plaintiff in this action]. I have personal knowledge of the following matters and could and would testify competently about them.

2. On or about _____ [date], I received a copy of Defendant's First Set of Demands for Production of

Electronically Stored Information in this action. A true and correct copy of that set of demands is attached to this declaration as Exhibit 1.

3. Demand No. 3 of that set of demands asks that I produce copies of all electronic mail sent or received by me, on my personal e-mail account during the nine-plus years that I was employed by Defendant, "regarding or relating to safety procedures at, or accidents or injuries occurring at, Defendant's rocket-engine testing facility."

4. My electronic mail service provider, Columbia Online, Inc., does not archive my e-mails. Electronic mail sent or received by me is programmatically saved to the hard drive of my personal computer. However, e-mails more than two weeks old can be searched only by fielded metadata: date, sender, recipient, and subject. Therefore, it is not possible to conduct an automated search of my saved e-mails for particular words or terms appearing in the body of an e-mail.

5. Because I often enter nothing at all in the subject line of an e-mail, or I enter "Message from John Smith" or words to that effect, it will not be possible for me to find all my e-mails that are responsive to Defendant's Demand No. 3 ("regarding or relating to safety procedures at, or accidents or injuries occurring at, Defendant's rocket-engine testing facility") by doing an automated search of subject lines. Instead, I will have to open and read each e-mail saved on my hard drive to decide whether it is responsive to Demand No. 3.

6. Over 20,000 e-mails sent or received by me during the nine-plus years covered by Demand No. 3 are saved on my computer and on an external drive. I estimate that the process of opening and reading them to ascertain which ones are responsive to Demand No. 3 will require at least 800 to 1,000 person-hours, assuming about 20 to 25 e-mails can be reviewed by one person per hour.

7. Most, if not all, of the e-mails sent to my personal e-mail account that are responsive to Defendant's Demand No. 3 are copies of e-mails that I sent or forwarded from the business e-mail account maintained for me by Defendant while I was an employee. I have no knowledge regarding Defendant's policies or procedures for saving or archiving e-mails sent or received by its employees using their business e-mail accounts.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Dated: _____

Respectfully submitted,

_____ [signature]

[typed name]

NOTES:

Authority:

CCP § 2031.060(b)

Checklist:

See 11.03

Discussion:

See 11.05, 11.06

Related Form for Motion and Notice of Motion:

See 11.20

Related Form for Order:

See *11.22*



41 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 11 Seeking or Opposing Protective Order
VI. FORMS

*1-11 MB Practice Guide: CA E-Discovery and Evidence 11.22***11.22 Protective Order.**

Protective Order.

SUPERIOR COURT OF CALIFORNIA,
COUNTY OF FARALLON

John Smith, Plaintiff, vs. Mary Jones Enterprises,
Inc., Defendant.

)
)
)
)
)

No. _____
PROTECTIVE ORDER

The motion of Plaintiff John Smith for an order providing that Plaintiff need not respond to Demand No. 3 of Defendant's First Set of Demands for Production of Electronically Stored Information came on regularly for hearing by the Court on _____ [date]. Plaintiff appeared by counsel Tom Doe; Defendant appeared by counsel Jane Lee.

The Court, having considered the declarations and other documents in support of and in opposition to the motion, having heard the arguments of counsel, and being fully advised in the matter, finds that the information sought in Demand No. 3 of Defendant's First Set of Demands is from a source that is not reasonably accessible because of undue burden and expense, and that there is not sufficient good cause for production of the information.

IT IS THEREFORE ORDERED that the motion be, and hereby is, granted, and that Plaintiff is not required to respond to Demand No. 3 of Defendant's First Set of Demands for Production of Electronically Stored Information.

[If imposing sanctions:]

IT IS FURTHER ORDERED that _____ [specify unsuccessful party and attorney, e.g., Defendant Mary Jones Enterprises, Inc., and its attorney Jane Lee] pay forthwith to _____ [specify successful party, e.g., Plaintiff John Smith] the sum of \$_____ as reasonable expenses and attorney's fees.

[OR, if not ordering sanctions:]

On further proof made to the satisfaction of the court that _____ [*specify unsuccessful party and attorney, e.g., Defendant Mary Jones Enterprises, Inc., and its attorney Jane Lee*] _____ [*acted with substantial justification or specify other circumstances making imposition of a sanction unjust*], IT IS FURTHER ORDERED that no monetary sanction be imposed on [*specify unsuccessful party and attorney, e.g., Defendant Mary Jones Enterprises, Inc., or its attorney Jane Lee*].

[*CONTINUE*]

Dated: _____
_____ [*signature*]

Judge of the Superior Court

NOTES:

Authority:

CCP § 2031.060(b)(1),(c)-(e), (h)

Checklist:

See 11.03

Discussion:

See 11.07

Related Form for Motion and Notice of Motion:

See 11.20

Related Declaration:

See 11.21



42 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.syn

§ 12.syn Synopsis to Chapter 12: Obtaining or Opposing Motion to Compel

12.01 Scope.

12.02 Objective and Strategy.

12.03 CHECKLIST: Moving to Compel Response to Demand for Production of Electronic Evidence.

12.04 Options and Strategies.

12.05 Movant Must Establish That Responding Party Failed to Serve Timely Response.

12.06 Movant May Establish That Responding Party Has Forfeited Objection to Demand.

12.06[1] Movant May Show That Responding Party's Late Response Was Not Adequate.

12.06[2] Movant May Show That Responding Party's Failure To Serve Timely Response Was Not Result of Mistake, Inadvertence, or Excusable Neglect.

12.07 Movant May Address Potential Sanctions.

12.07[1] Movant May Request Sanctions Against Responding Party.

12.07[2] Movant May Oppose Responding Party's Request for Sanctions.

12.08 CHECKLIST: Opposing Motion to Compel Response to Demand for Production of Electronic Evidence.

12.09 Options and Strategies.

12.10 Responding Party May Contest Ground for Motion.

12.11 Responding Party May Seek Relief From Forfeiture of Objections to Demand for Production.

12.11[1] Responding Party Should Ascertain Whether Grounds for Objection Exist.

12.11[2] Responding Party May Establish That Adequate, Though Untimely, Response Was Served.

12.11[3] Responding Party May Establish That Failure to Serve Timely Response Was Result of Mistake, Inadvertence, or Excusable Neglect.

12.12 Responding Party May Address Potential Sanctions.

12.12[1] Responding Party May Oppose Movant's Request for Sanctions.

12.12[2] Responding Party May Request Sanctions Against Unsuccessful Movant.

12.13 CHECKLIST: Moving to Compel Further Response to Demand for Production of Electronic Evidence.

12.14 Options and Strategies.

12.15 Propounding Party Should Determine Whether Grounds Exist for Order Compelling Further Response.

12.15[1] Propounding Party Should Ascertain Whether Statement of Compliance Is Incomplete.

12.15[2] Propounding Party Should Ascertain Whether Representation of Inability to Comply Is Inadequate, Incomplete, or Evasive.

12.15[3] Propounding Party Should Ascertain Whether Objection to Request Is Without Merit or Too General.

12.15[4] Propounding Party Should Ascertain Existence of Good Cause for Production of Electronic Evidence.

12.15[5] Propounding Party Should Ascertain Whether Responding Party Will Produce Electronic Evidence in Reasonably Usable Form.

12.15[6] Propounding Party Should Verify That Response Has Been Signed Under Oath by Appropriate Individual.

12.15[7] Counsel for Propounding Party Must Meet and Confer With Opposing Counsel Before Making Motion.

12.16 Counsel Must Ensure Compliance With Special Requirements for Motion.

12.16[1] Motion Must Set Forth Specific Facts Showing Good Cause for Discovery.

12.16[2] Motion Must Include Meet-and-Confer Declaration.

12.16[3] Separate Statement Must Accompany Motion.

12.16[4] Motion Must Be Filed by Statutory Deadline.

12.17 Movant May Address Potential Sanctions.

12.17[1] Movant May Request Sanctions Against Responding Party.

12.17[2] Movant May Oppose Responding Party's Request for Sanctions.

12.18 CHECKLIST: Opposing Motion to Compel Further Response.

12.19 Options and Strategies.

12.20 Responding Party May Contest Grounds for Motion.

12.20[1] Responding Party May Establish That Statement of Compliance Is Complete.

12.20[2] Responding Party May Establish Inability to Comply With Demand.

12.21 Responding Party May Assert Affirmative Defenses to Motion.

12.21[1] Responding Party May Establish That Movant Forfeited Right to Compel Further Response by Waiting More Than 45 Days to Serve Motion.

12.21[2] Responding Party May Establish That Electronic Evidence Sought by Movant Is Not Reasonably Accessible.

12.21[3] Responding Party May Establish Grounds for Objections to Demand.

12.21[4] Responding Party May Establish Grounds to Limit Discovery.

12.22 Responding Party May Address Potential Sanctions.

12.22[1] Responding Party May Oppose Movant's Request for Sanctions.

12.22[2] Responding Party May Request Sanctions Against Unsuccessful Movant.

12.23 CHECKLIST: Moving to Compel Compliance With Statement of Compliance.

12.24 Options and Strategies.

12.25 Movant Must Establish That Responding Party Has Failed to Produce Electronic Evidence in Accordance With Statement of Compliance.

12.26 Counsel Must Prepare Separate Statement to Accompany Motion.

12.27 Movant May Address Potential Sanctions.

12.27[1] Movant May Request Sanctions Against Responding Party.

12.27[2] Movant May Oppose Responding Party's Request for Sanctions.

12.28 CHECKLIST: Opposing Motion to Compel Compliance With Statement of Compliance.

12.29 Options and Strategies.

12.30 Responding Party Should Establish That Electronic Evidence Has Been Produced in Accordance With Statement of Compliance.

12.31 Responding Party May Address Potential Sanctions.

12.31[1] Responding Party May Oppose Movant's Request for Sanctions.

12.31[2] Responding Party May Request Sanctions Against Unsuccessful Movant.

- 12.32 Notice of Motion and Motion to Compel Response to Demand for Production of Electronic Evidence.
- 12.33 Declaration Supporting Motion to Compel Response to Demand for Production of Electronic Evidence.
- 12.34 Declaration Opposing Motion to Compel Response to Demand for Production of Electronic Evidence.
- 12.35 Order Compelling Response to Demand for Production of Electronic Evidence.
- 12.36 Notice of Motion and Motion to Compel Further Response to Demand for Production of Electronic Evidence.
- 12.37 Declaration Supporting Motion to Compel Further Response to Demand for Production of Electronic Evidence.
- 12.38 Order Compelling Further Response to Demand for Production of Electronic Evidence.
- 12.39 Notice of Motion and Motion to Compel Compliance With Statement of Compliance.
- 12.40 Declaration Supporting Motion to Compel Compliance With Statement of Compliance.
- 12.41 Order Compelling Compliance With Statement of Compliance.



43 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

I. STRATEGY

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.01

12.01 Scope.

This chapter covers:

- Moving to compel a response to a demand for the production of electronically stored information [see 12.03-12.07; *Forms*: 12.32, 12.33, 12.35].
- Opposing a motion to compel a response to a demand for the production of electronically stored information [see 12.08-12.12; *Form*: 12.34].
- Moving to compel a further response to a demand for the production of electronically stored information [see 12.13-12.17; *Forms*: 12.36-12.38].
- Opposing a motion to compel a further response to a demand for the production of electronically stored information [see 12.18-12.22].
- Moving to compel compliance with a demand for the production of electronically stored information [see 12.23-12.27; *Forms*: 12.39-12.41].
- Opposing a motion to compel compliance with a demand for the production of electronically stored information [see 12.28-12.31].

This chapter does not cover the procedures for formulating and serving demands for the production of electronic evidence. For discussion of those procedures, see *Ch. 6, Demanding Production of Electronically Stored Information in California Court*, 6.09-6.13.

This chapter does not cover the procedures for responding to a demand for the production of electronic evidence. For discussion of those procedures, see *Ch. 8, Responding to Electronic Discovery Requests in California*, 8.12-8.23.

This chapter does not cover the procedures for opposing a demand for the production of electronic evidence. For discussion of those procedures, see *Ch. 10, Opposing Demands for Production of Electronic Evidence in California Court*.

This chapter does not cover the procedures for seeking or opposing a protective order. For discussion of those procedures, see *Ch. 11, Seeking or Opposing Protective Order, 11.03-11.12*

Core Statutes:

CCP §§ 2031.300, 2031.310, 2031.320



44 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

I. STRATEGY

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.02

12.02 Objective and Strategy.

A propounding party who is dissatisfied with the responding party's response to a demand for production of electronically stored information may seek assistance of the court through three kinds of motions:

- First, if no response has been served, the propounding party may move to compel a response [*CCP* § 2031.300].
- Second, if a response is served but the propounding party deems the response deficient or disputes an objection or claim of privilege asserted by the responding party, the propounding party may move for an order compelling a further response [*CCP* § 2031.310].
- Finally, even if disputes over objections and claimed privilege have not arisen or have been resolved by the court, the propounding party may move for an order compelling compliance with the response if the responding party fails to produce the demanded information in accordance with the response [*CCP* § 2031.320].

Cross References:

Moving to compel response, see 12.03-12.07.

Opposing motion to compel response, see 12.08-12.12.

Moving to compel further response, see 12.13-12.17.

Opposing motion to compel further response, see 12.18-12.22.

Moving to compel compliance with response, see 12.23-12.27.

Opposing motion to compel compliance with response, see 12.28-12.31.



45 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

II. MOVING TO COMPEL RESPONSE TO DEMAND FOR PRODUCTION OF ELECTRONIC EVIDENCE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.03

12.03 CHECKLIST: Moving to Compel Response to Demand for Production of Electronic Evidence.

☐ Verify that party to whom demand for production of electronically stored information is directed has failed to serve timely response.

Authority:

CCP §§ 2031.260(a), 2031.300(b)

Discussion:

See 12.05

☐ Review office file and court docket to determine whether court has entered order setting deadline for response to demand for production; if so, verify that response was not served on or before deadline.

Authority:

CCP § 2031.260(a), (b)

☐ In unlawful detainer case, if court has not set deadline for response, verify that no response was served within five days after service of demand for production.

Authority:

CCP § 2031.260(b)

☐ In any other case, if court has not set deadline for response, verify that no response was served within 30 days after service of demand for production.

Authority:

CCP § 2031.260(a)

- ☐ Consider meeting and conferring with opposing counsel to attempt to resolve issues informally, even though "meet and confer" declaration is not required for motion to compel when no response has been served.

Authority:

CCP § 2031.300(b)

Discussion:

See 12.04

- ☐ Prepare necessary documents for motion to compel response.
- ☐ Prepare notice of motion and motion to compel response to demand for production, including request for declaration that objections to demand have been forfeited or waived, and request for monetary sanctions.

Authority:

CCP § 2031.300(b), (c); Cal Rules Ct, Rules 3.1110, 3.1112(a)

Discussion:

See 12.06, 12.07[1]

Form:

See 12.32

- ☐ Prepare memorandum in support of motion.

Authority:

Cal Rules Ct, Rules 3.1112(a)(3), 3.1113

- ☐ Prepare affidavits or declarations, along with any appropriate exhibits, that are necessary to provide factual support for motion.

Authority:

Cal Rules Ct, Rule 3.1112(b)

Form:

See 12.33

- ☐ Prepare proposed order.

Authority:

Cal Rules Ct, Rule 3.1112(b)

Form:

See 12.35

- ☐ Follow standard procedure for noticed motion.

Authority:

Cal Rules Ct, Rule 3.1300 et seq.

Discussion:

See Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure, Ch. 26, Law and Motion Procedure, 26.39

☐ If motion is denied, demonstrate that moving party acted with substantial justification or that other circumstances make imposition of sanctions on moving party unjust.

Authority:

CCP § 2031.300(c)

Discussion:

See 12.07[2]



46 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

II. MOVING TO COMPEL RESPONSE TO DEMAND FOR PRODUCTION OF ELECTRONIC EVIDENCE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.04

12.04 Options and Strategies.

If the party to whom a demand for production is directed does not serve a timely response, the propounding party may move for an order compelling a response [CCP § 2031.300(b)]. An important consequence of a party's failure to serve a timely response is the forfeiture (called "waiver" in the statute) of objections to the demand, although the court may relieve the party of the forfeiture under some circumstances [CCP § 2031.300(a)].

Strategic Point:



A forfeiture of objections does not occur when the response is timely but inadequate. Although the use of boilerplate objections based on privilege or attorney work product protection may warrant other sanctions, the use of such objections does not work a forfeiture as long as the response is timely [*People ex rel. Lockyer v. Superior Court* (2004) 122 CA4th 1060, 1074-1075, 19 CR3d 324] .



Cross Reference:

Discussion of forfeiture of objections, see 12.06, 12.11.



Strategic Point--Contact Opposing Counsel May Be Productive Even Though No Formal "Meet and

Confer" Requirement Exists:

Unlike a motion to compel a *further* response, a motion to compel an initial response need not be preceded by an attempt to settle the matter informally, and no "meet and confer" declaration need accompany the motion [compare CCP § 2031.300(b) with CCP § 2031.310(b)(2); see also CCP § 2016.040]. However, counsel should nevertheless attempt to contact opposing counsel to determine if the failure to respond was an oversight that can be remedied quickly and cost-effectively without a formal motion. Even if the matter is not resolved informally, offering opposing counsel the opportunity to rectify the failure to respond can lay the groundwork for an award of sanctions if a motion becomes necessary to obtain a response [see CCP § 2031.300(c)].



Cross Reference:

Discussion of sanctions, see 12.07; see also Ch. 13, Seeking or Opposing Sanctions for Noncompliance.

The moving papers for a motion to compel a response include a motion and notice of motion, one or more declarations establishing the factual basis for the motion, and a memorandum in support of the motion [*see Cal Rules of Ct, Rule 3.1112(a), (b)*]. A "separate statement" of information describing the discovery requests and responses at issue, which must accompany most discovery motions, is not required for a motion to compel a response when no response has been provided [*Cal Rules of Ct, Rule 3.1345(b)*].



47 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

II. MOVING TO COMPEL RESPONSE TO DEMAND FOR PRODUCTION OF ELECTRONIC EVIDENCE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.05

12.05 Movant Must Establish That Responding Party Failed to Serve Timely Response.

The party to whom a demand for production of electronically stored information is directed ordinarily must serve a response to the demand within 30 days after service of the demand [CCP § 2031.260(a)]. If a timely response is not served, the propounding party may move for an order compelling a response [CCP § 2031.300(b)].

Exceptions:

In an unlawful detainer action or similar proceeding [see CCP § 1159 *et seq.*], the usual time to respond is five days after service of the demand [CCP § 2031.260(b)]. In any case, however, the court may, on motion by the propounding or responding party, shorten or extend the time for responding to the demand [CCP § 2031.260(a), (b)]. In any case, the parties may agree in writing to an extended date for serving a response [CCP § 2031.270(a), (c)].



Strategic Point:

Unless the agreement expressly states otherwise, the parties' agreement to extend the date for a response does not prevent the responding party from asserting any objection or privilege claim that it could have asserted in a response that is served within the statutory deadline [CCP § 2031.270(c)].



Cross Reference:

Responding to demand for production of electronically stored information, see *Ch. 8, Responding to Electronic Discovery Requests*, 8.12-8.23.



48 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

II. MOVING TO COMPEL RESPONSE TO DEMAND FOR PRODUCTION OF ELECTRONIC EVIDENCE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.06

12.06 Movant May Establish That Responding Party Has Forfeited Objection to Demand.

12.06[1] Movant May Show That Responding Party's Late Response Was Not Adequate. A failure to serve a timely response to a demand for production of electronically stored information ordinarily works a forfeiture (called "waiver" in the statute) of any objection to the demand, including one based on privilege or on work product protection [*CCP* § 2031.300(a); see *CCP* § 2018.010 et seq.]. The party to whom the demand is directed may move the court for relief from this forfeiture, but the court may not grant the motion unless the party seeking relief has served a response that, except for being untimely, substantially complies with the requirements for a response [*CCP* § 2031.300(a)(1)].

12.06[2] Movant May Show That Responding Party's Failure To Serve Timely Response Was Not Result of Mistake, Inadvertence, or Excusable Neglect. A failure to serve a timely response to a demand for production of electronically stored information ordinarily works a forfeiture (called "waiver" in the statute) of any objection to the demand, including one based on privilege or on work product protection [*CCP* § 2031.300(a); see *CCP* § 2018.010 et seq.]. The party to whom the demand is directed may move the court for relief from this forfeiture, but the court may not grant the motion unless the party's failure to serve a timely response was the result of mistake, inadvertence, or excusable neglect [*CCP* § 2031.300(a)(2)].

Cross Reference:

Discussion of standard for assessing mistake, inadvertence, and excusable neglect, see 12.11[3].



49 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

II. MOVING TO COMPEL RESPONSE TO DEMAND FOR PRODUCTION OF ELECTRONIC EVIDENCE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.07

12.07 Movant May Address Potential Sanctions.

12.07[1] Movant May Request Sanctions Against Responding Party. The court ordinarily *must* impose a monetary sanction against any party, person, or attorney who unsuccessfully opposes a motion to compel a response to a demand for production of electronically stored information [*CCP* § 2031.300(c); *see CCP* § 2023.010 *et seq.*; *see also Cal Rules Ct, Rule 3.1348(a)* (sanction may be imposed even if no formal opposition to motion was filed)].

Exceptions:

The court is not required to impose a monetary sanction if it finds that the party, person, or attorney subject to the sanction acted with substantial justification or that other circumstances make the imposition of the sanction unjust [*CCP* § 2031.300(c)]. Furthermore, absent exceptional circumstances, the court may not impose sanctions on a party or any attorney for failure to provide electronically stored information that has been lost, damaged, altered, or overwritten as a result of the routine, good-faith operation of an electronic information system [*CCP* § 2031.300(d)(1)].

12.07[2] Movant May Oppose Responding Party's Request for Sanctions. If the court denies the motion to compel a response to the demand for production of electronically stored information, the court ordinarily *must* impose a monetary sanction against the moving party and his or her attorney [*CCP* § 2031.300(c); *see CCP* § 2023.010 *et seq.*].

The moving party may avoid sanctions, however, by establishing that the moving party (or his or her attorney) acted with substantial justification or that other circumstances make the imposition of the sanction unjust [*CCP* § 2031.300(c)].



50 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

III. OPPOSING MOTION TO COMPEL RESPONSE TO DEMAND FOR PRODUCTION OF ELECTRONIC EVIDENCE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.08

12.08 CHECKLIST: Opposing Motion to Compel Response to Demand for Production of Electronic Evidence.

- ☐ Obtain documentation of any agreement between parties establishing time for response beyond times specified by statute.

Authority:

CCP § 2031.270

Discussion:

See 12.10

- ☐ If grounds exist for objection to demand, take steps to establish grounds for court order granting relief from forfeiture of objections.

Authority:

CCP § 2031.300(a)

Discussion:

See 12.11

- ☐ If late response to demand has been served, verify that response complies with all applicable statutory requirements other than timeliness.
- ☐ If no response to demand has been served, prepare response that complies with all applicable statutory requirements other than timeliness, and serve response before hearing on motion to compel response.
- ☐ Ascertain facts demonstrating that failure to serve timely response was result of

mistake, inadvertence, or excusable neglect.

☐ Prepare papers opposing motion.

☐ Prepare memorandum opposing motion, including as appropriate:

Authority:

Cal Rules Ct, Rules 3.1112(a)(3), 3.1113

☐ Request for relief from forfeiture or waiver of objections to demand.

Authority:

CCP § 2031.300(a)

Discussion:

See 12.11

☐ Request for monetary sanction.

Authority:

CCP § 2031.300(c)

Discussion:

See 12.12[2]

☐ Prepare affidavits or declarations, along with any appropriate exhibits, that are necessary to provide factual support for opposition.

Authority:

Cal Rules Ct, Rules 3.1112(b)

Form:

See 12.34

☐ Follow standard procedure for opposing noticed motion.

Authority:

Cal Rules Ct, Rule 3.1300 et seq.

Discussion:

See *Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure, Ch. 26, Law and Motion Procedure, 26.46*

☐ If motion is granted, demonstrate either of following:

Authority:

CCP § 2031.300(c)

Discussion:

See 12.12[1]

- ☐ Opposing party acted with substantial justification.
- ☐ Other circumstances make imposition of sanctions on opposing party unjust.



51 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

III. OPPOSING MOTION TO COMPEL RESPONSE TO DEMAND FOR PRODUCTION OF ELECTRONIC EVIDENCE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.09

12.09 Options and Strategies.

An important consequence of a party's failure to serve a timely response to a demand for production is the forfeiture (called "waiver" in the statute) of objections to the demand. However, the court may grant relief from the forfeiture if (1) the party seeking relief has served a response to the demand that, except for being untimely, substantially complies with the requirements for a response; and (2) the party's failure to serve a timely response was the result of mistake, inadvertence, or excusable neglect [*CCP* § 2031.300(a)]. Accordingly, as soon as counsel becomes aware that a deadline for responding to a production demand has been missed, counsel should (1) prepare and serve an adequate response to the demand, including any applicable objections; and (2) prepare to make a showing of any mistake, inadvertence, or excusable neglect that resulted in the failure to serve a timely response.

Decision Point:

Although relief from the forfeiture of objections typically is sought in response to the propounding party's motion to compel, counsel may decide to move the court for relief from the forfeiture, without waiting for the propounding party to seek an order compelling a response [*see CCP* § 2031.300(a)].



Warning:

Missing a deadline for response is very bad. If the court does not grant relief from the forfeiture of objections, counsel's failure to serve a timely response to a production demand may be the basis for a malpractice claim. Accordingly, counsel should ensure that adequate office procedures are in place to calendar response dates, document any extensions granted by the court or the propounding party's counsel, and accomplish timely service of responses.



Cross Reference:

Responding to demand for production of electronically stored information, see *Ch. 8, Responding to Electronic Discovery Requests in California*, 8.12-8.23.



52 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

III. OPPOSING MOTION TO COMPEL RESPONSE TO DEMAND FOR PRODUCTION OF ELECTRONIC EVIDENCE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.10

12.10 Responding Party May Contest Ground for Motion.

A party opposing a motion to compel a response to a demand for production of electronically stored information may contest the ground for the motion (i.e., that no timely response to the demand was served). For example, if the parties agreed to a later date for response, and a response was served by that later date, opposition to a motion to compel a response to a demand for production may be based on a showing that an agreement of the parties sets a time for response beyond the times specified by statute [*see CCP § 2031.270(a)*]. Such an agreement may be informal, but it must be confirmed in a writing that specifies the extended date for production or for service of a response [*CCP § 2031.270(b)*]. Unless the agreement expressly states otherwise, it is effective to preserve the responding party's right to respond to any item or category of item in the demand to which the agreement applies, in any manner permitted by statute, including objections [*CCP § 2031.270(c)*; *see CCP §§ 2031.210, 2031.220, 2031.230, 2031.240, 2031.280*].



53 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

III. OPPOSING MOTION TO COMPEL RESPONSE TO DEMAND FOR PRODUCTION OF ELECTRONIC EVIDENCE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.11

12.11 Responding Party May Seek Relief From Forfeiture of Objections to Demand for Production.

12.11[1] Responding Party Should Ascertain Whether Grounds for Objection Exist. A failure to serve a timely response to a demand for production of electronically stored information ordinarily constitutes a forfeiture (called "waiver" in the statute) of any objection to the demand [CCP § 2031.300(a); see CCP § 2031.210(a)(3)].



Strategic Point:

A forfeiture of objections does not occur when the response is timely but inadequate. Although the use of boilerplate objections based on privilege or attorney work product protection may warrant other sanctions, the use of such objections does not work a forfeiture so long as the response is timely [*People ex rel. Lockyer v. Superior Court* (2004) 122 CA4th 1060, 1074-1075, 19 CR3d 324] .

The party to whom the demand is directed may respond to a motion to compel a response by asking the court for relief from the forfeiture, if grounds for objection exist [CCP § 2031.300(a)]. Grounds for objection include the following:

- The information sought is protected by attorney-client privilege [see CCP § 2031.300(a); see also CCP § 2031.285].
- The information sought is protected as attorney work product [see CCP § 2031.300(a); see also CCP § 2018.010 et seq., CCP § 2031.285].
- The information sought is from a source that is not reasonably accessible because of undue burden or expense [CCP § 2031.210(d)].
- The party is unable to comply with the demand, because the particular item or category has never existed; has been destroyed; has been lost, misplaced, or stolen; or has never been, or is no longer, in the possession, custody, or control of the party [CCP § 2031.230].
- The demand for production is premature; i.e., served fewer than 10 days after the earlier of service of

the summons on, or appearance by, the party to whom the demand is directed [*see CCP § 2031.020(b)*].

Exceptions:

In an unlawful detainer action or similar proceeding [*see CCP § 1159 et seq.*], a demand for production may be served as soon as five days after the earlier of service of the summons on, or appearance by, the party to whom the demand is directed [*CCP § 2031.020(c)*]. In any case, however, the court, for good cause shown, may shorten the time for serving a demand for production [*CCP § 2031.020(d)*].

■ The demand for production fails to comply with applicable statutory requirements, by (1) not specifically describing each individual item or reasonably particularizing each category of item; (2) not specifying a reasonable time for production that is least 30 days after service of the demand; (3) not specifying a reasonable place for production; or (4) not specifying the manner in which inspection, copying, testing, sampling, or related activity will be performed, and whether that activity will permanently alter or destroy the item involved [*CCP § 2031.030(c)*].

Exceptions:

In an unlawful detainer action or similar proceeding [*see CCP § 1159 et seq.*], a demand for production may specify a time for production that is as soon as five days after service of the demand [*CCP § 2031.030(c)(2)*]. In any case, however, the court, for good cause shown, may grant leave to specify an earlier time for production [*CCP § 2031.030(c)(2)*].

■ The demand for production is a supplemental demand that exceeds the limitations applicable to such demands. Generally, a party may propound a supplemental demand for production of electronically stored information acquired by the responding party after responding to the initial demand [*CCP § 2031.050(a)*]. However, unless otherwise ordered by the court for good cause shown, supplemental demands may be made no more than twice before the initial setting of a trial date, and, subject to the time limits generally applicable to discovery proceedings and motions [*see CCP § 2024.010 et seq.*], no more than once after the initial setting of a trial date [*CCP § 2031.050(b), (c)*].



Warning:

The court may grant relief from the forfeiture of objections only if (1) the party seeking relief has served a response to the demand that, except for being untimely, substantially complies with the requirements for a response, and (2) the party's failure to serve a timely response was the result of mistake, inadvertence, or excusable neglect [*CCP § 2031.300(a)*].



Cross References:

Discussion of adequate but untimely response, see 12.11[2].

Discussion of establishing mistake, inadvertence, or excusable neglect, see 12.11[3].

12.11[2] Responding Party May Establish That Adequate, Though Untimely, Response Was Served. To obtain relief from a forfeiture of objections resulting from a failure to serve a timely response to a demand for production, the party to whom the demand was directed must establish that he or she subsequently served an adequate response, that is, one that substantially complied with the requirements for a response [*CCP § 2031.300(a)(1)*; *see CCP §§ 2031.210, 2031.220, 2031.230, 2031.240, 2031.280*]. In addition to meeting certain formal requirements [*see CCP § 2031.210(b), (c)*], a response to a demand for production must separately address each item or category of item sought, by a statement that the responding party will comply with the demand, a representation that the party lacks the ability to comply with the demand, or an objection to the demand [*CCP § 2031.210(a)*]. If the responding party objects to the discovery of electronically stored information on the grounds that it is from a source that is not reasonably accessible

because of undue burden or expense and that the responding party will not search the source in the absence of an agreement with the propounding party or court order, the responding party must identify in its response the types or categories of sources of electronically stored information that it asserts are not reasonably accessible [CCP § 2031.210(d)].



Cross Reference:

Responding to demand for production of electronically stored information, see *Ch. 8, Responding to Electronic Discovery Requests in California*, 8.12-8.23.

12.11[3] Responding Party May Establish That Failure to Serve Timely Response Was Result of Mistake, Inadvertence, or Excusable Neglect. To obtain relief from a forfeiture of objections resulting from a failure to serve a timely response to a demand for production, the party to whom the demand was directed must establish that the failure to serve a timely response was the result of mistake, inadvertence, or excusable neglect [CCP § 2031.300(a)(2)]. In deciding whether a failure to serve a timely response was the result of mistake, inadvertence, or excusable neglect, the court will apply the same standard as that used in determining whether to grant relief from judgment under CCP § 473(b) [*City of Fresno v. Superior Court* (1988) 205 CA3d 1459, 1467, 253 CR 296] .

Examples--Relief Not Justified:

- Counsel's mistake of law on a relatively simple and undebatable matter is not a valid ground for relief, nor is the fact that counsel is very busy [*City of Fresno v. Superior Court* (1988) 205 CA3d 1459, 1467, 253 CR 296] .

- Similarly, a tactical choice made by counsel does not constitute mistake, inadvertence, or excusable neglect. Thus, counsel's failure to assert the attorney-client privilege in reliance on potential relief from an ultimately unsuccessful motion for a protective order was deemed a tactical choice to pursue a certain course of action, rather than a mistake or excusable neglect [*Scottsdale Ins. Co. v. Superior Court* (1997) 59 CA4th 263, 274-276, 69 CR2d 112] .



54 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

III. OPPOSING MOTION TO COMPEL RESPONSE TO DEMAND FOR PRODUCTION OF ELECTRONIC EVIDENCE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.12

12.12 Responding Party May Address Potential Sanctions.

12.12[1] Responding Party May Oppose Movant's Request for Sanctions. If the court grants the motion to compel a response to the demand for production of electronically stored information, the court ordinarily must impose a monetary sanction on the opposing party and his or her attorney [*CCP § 2031.300(c)*; *see CCP § 2023.010 et seq.*; *see also Cal Rules Ct, Rule 3.1348(a)* (sanction may be imposed even if no formal opposition to motion was filed)]. However, the opposing party may avoid sanctions by establishing either of the following:

- The opposing party (or his or her attorney) acted with substantial justification [*CCP § 2031.300(c)*].
- Other circumstances make the imposition of the sanction unjust [*CCP § 2031.300(c)*].



Strategic Point:

Only monetary sanctions are available for unsuccessfully opposing an initial motion to compel a response to a demand for production; other sanctions, such as issue sanctions, evidence sanctions, or terminating sanctions [*see CCP § 2023.010 et seq.*] are available only if the party to be sanctioned has failed to obey an order compelling a response [*CCP § 2031.300(c)*].

12.12[2] Responding Party May Request Sanctions Against Unsuccessful Movant. The court ordinarily must impose a monetary sanction [*see CCP § 2023.010 et seq.*] against any party, person, or attorney who unsuccessfully makes a motion to compel a response to a demand for production of electronically stored information [*CCP § 2031.300(c)*].

Exception:

The court is not required to impose a monetary sanction if it finds that the party, person, or attorney subject to the sanction acted with substantial justification or that other circumstances make the imposition of the sanction unjust [*CCP § 2031.300(c)*].



55 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

IV. MOVING TO COMPEL FURTHER RESPONSE TO DEMAND FOR PRODUCTION OF ELECTRONIC EVIDENCE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.13

12.13 CHECKLIST: Moving to Compel Further Response to Demand for Production of Electronic Evidence.

☐ Determine whether grounds exist for order compelling further response to demand for production of electronically stored information.

☐ Determine whether response to demand is incomplete.

Authority:

CCP § 2031.310(a)(1)

Discussion:

See 12.15[1]

☐ Determine whether representation of inability to comply with demand is inadequate, incomplete, or evasive.

Authority:

CCP § 2031.310(a)(2)

Discussion:

See 12.15[2]

☐ Determine whether any objection asserted in response is without merit or too general.

Authority:

CCP § 2031.310(a)(3)

Discussion:

See 12.15[3]

- ☐ Determine whether there is good cause for discovery of information sought by demand.

Authority:

CCP §§ 2031.060(c)-(e), 2031.310(b)(1)

Discussion:

See 12.15[4]

- ☐ Determine whether response indicates that information will not be produced in usable form.

Authority:

CCP § 2031.280(c)-(e)

Discussion:

See 12.15[5]

- ☐ Determine whether signature of appropriate individual has been omitted from response.

Authority:

CCP § 2031.250

Discussion:

See 12.15[6]

- ☐ Meet and confer with opposing counsel to attempt to resolve issues informally.

Authority:

CCP §§ 2031.310(b)(2), 2016.040

Discussion:

See 12.16[2]

- ☐ Prepare necessary documents for motion to compel further response.

- ☐ Prepare notice of motion and motion to compel response to demand for production, including request for monetary sanctions.

Authority:

CCP § 2031.310(a), (h); Cal Rules Ct, Rules 3.1110, 3.1112(a)

Discussion:

See 12.17[1]

Form:

See 12.36

- ☐ Prepare memorandum in support of motion.

Authority:

Cal Rules Ct, Rules 3.1112(a)(3), 3.1113

- ☐ Prepare affidavits or declarations, along with any appropriate exhibits, setting forth specific facts showing good cause justifying discovery sought by demand.

Authority:

CCP § 2031.310(b)(1); Cal Rules Ct, Rule 3.1112(b)

Discussion:

See 12.16[1]

- ☐ Prepare "meet-and-confer" declaration.

Authority:

CCP §§ 2031.310(b)(2), 2016.040

Discussion:

See 12.16[2]

- ☐ Prepare "separate statement" providing all information necessary to understand each demand and all responses to it that are at issue.

Authority:

Cal Rules Ct, Rule 3.1345(a), (c)

Discussion:

See 12.16[3]

- ☐ Prepare proposed order.

Authority:

Cal Rules Ct, Rule 3.1112(b)

Form:

See 12.38

- ☐ Follow standard procedure for noticed motion, ensuring that notice of motion is given within 45 days after service of response to demand, or on or before any later date established by parties' written agreement.

Authority:

CCP § 2031.310(c); Cal Rules Ct, Rule 3.1300 et seq.

Discussion:

See 12.16[4]; see also *Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure, Ch. 26, Law and Motion Procedure*, 26.39 (checklist for standard motion procedure).

- ☐ If motion is denied, demonstrate that moving party acted with substantial justification or that other circumstances make imposition of sanctions on moving party unjust.

Authority:

CCP § 2031.310(h)

Discussion:

See 12.17[2]



56 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel
 IV. MOVING TO COMPEL FURTHER RESPONSE TO DEMAND FOR PRODUCTION OF ELECTRONIC
 EVIDENCE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.14

12.14 Options and Strategies.

The propounding party may, within 45 days after service of a response to a demand for production, move to compel a further response if the initial response contains (1) an incomplete statement of compliance with any item of the demand; (2) a representation of inability to comply is inadequate, incomplete, or evasive; or (3) an objection in the response is without merit or too general [CCP § 2031.310(a), (c)].

Distinguish--Motion to Compel Compliance:

The purpose of a motion to compel a further response is to obtain a response that completely identifies and requires the production of the available, nonprivileged documents. Once an adequate response has been obtained, there is no longer any dispute over the right to have the items produced, and any subsequent refusal to produce the items as promised will lead to a motion to compel compliance [*Standon Co., Inc. v. Superior Court* (1990) 225 CA3d 898, 903, 275 CR 833] . Thus, a distinctive feature of the motion to compel a further response is the statutory deadline for the motion, which effectively requires that any nonmeritorious claim of privilege be attacked and resolved by a motion made within 45 days of its service [CCP § 2031.310(c)]. A motion to compel compliance, in contrast, is not subject to any statutory time limit other than the generally applicable requirement that all discovery motions be heard on or before the 15th day before the date initially set for trial [*Standon Co., Inc. v. Superior Court* (1990) 225 CA3d 898, 903, 275 CR 833 ; see CCP § 2031.320(a); see also CCP § 2024.020(a)]. That generally applicable cutoff for the hearing of discovery motions can be extended by agreement of the parties, or by the court in its case management order or in response to a party's motion [see CCP §§ 2024.050, 2024.060; *Cal Rules Ct, Rule 3.728*; see also *Cal Rules Ct, Rules 3.724, 3.727*].

Cross Reference:

Discussion of motion to compel compliance, see 12.23-12.27.

The moving papers for a motion to compel a further response include a motion and notice of motion, one or more declarations establishing the factual basis for the motion and setting forth specific facts showing good cause to justify the discovery sought by the demand, a "separate statement" of information describing the discovery requests and responses at issue, a meet-and-confer declaration, and a memorandum in support of the motion [CCP §§ 2016.040, 2031.310(b); *Cal Rules of Ct, Rules 3.1112(a), (b), 3.1345(a)(3)*].

► **Cross References:**

Discussion of necessary elements of motion, see *12.16*.

Forms, see *12.36*, *12.37*.



57 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel
 IV. MOVING TO COMPEL FURTHER RESPONSE TO DEMAND FOR PRODUCTION OF ELECTRONIC
 EVIDENCE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.15

12.15 Propounding Party Should Determine Whether Grounds Exist for Order Compelling Further Response.

12.15[1] Propounding Party Should Ascertain Whether Statement of Compliance Is Incomplete. A party receiving a demand for the production of electronically stored information may respond to any particular item or category of item with a statement that the party will comply with that demand [CCP § 2031.210(a)(1)]. The statement of compliance must state that (1) the production (or the inspection, copying, testing, sampling, or related activity specified in the demand) will be allowed, either in whole or in part; and (2) all documents or things in the demanded category that are in the possession, custody, or control of that party and to which no objection is being made will be included in the production [CCP § 2031.220]. If the statement of compliance omits any of this required information, the propounding party may move for an order compelling a further response to the demand [CCP § 2031.310(a)(1)].

12.15[2] Propounding Party Should Ascertain Whether Representation of Inability to Comply Is Inadequate, Incomplete, or Evasive. A party receiving a demand for the production of electronically stored information may respond to any particular item or category of item with a representation that the party lacks the ability to comply with the demand for production (or inspection, copying, testing, or sampling) of that particular item or category of item [CCP § 2031.210(a)(2)]. A representation of inability to comply must (1) affirm that a diligent search and a reasonable inquiry have been made in an effort to comply with that demand; (2) specify whether the inability to comply is because the particular item or category never existed, has been destroyed, has been lost, misplaced, or stolen, or has never been, or is no longer, in the possession, custody, or control of the party making the representation; and (3) set forth the name and address of any natural person or organization known or believed by that party to have possession, custody, or control of that item or category of item [CCP § 2031.230]. If the representation of inability to comply is inadequate, incomplete, or evasive, the propounding party may move for an order compelling a further response to the demand [CCP § 2031.310(a)(2)].

12.15[3] Propounding Party Should Ascertain Whether Objection to Request Is Without Merit or Too General. If an objection to a demand for production of electronically stored information is without merit or too general, the propounding party may move for an order compelling a further response [CCP § 2031.310(a)(3)].

An objection to a demand may be deemed too general if it does not separately address in particular each item or category of items specified in the demand [CCP § 2031.210(a)(3)].

If the responding party objects on the ground that the demanded information is from a source that is not reasonably accessible because of undue burden or expense and that the responding party will not search the source in the absence of an agreement with the propounding party or a court order, the response must identify the types or categories of sources of electronically stored information that it asserts are not reasonably accessible [CCP § 2031.210(d)].

An objection to a demand for production of an item or category of item must do both of the following [CCP § 2031.240(b)]:

- Identify with particularity any electronically stored information falling within any category of item in the demand to which the objection is being made.
- Set forth clearly the extent of, and the specific ground for, the objection.

Examples:

- If the objection is based on a claim of privilege, the particular privilege must be identified [CCP § 2031.240(b)(2)].
- If an objection is based on a claim that the information sought is protected work product [see CCP § 2018.010 *et seq.*], that claim must be expressly asserted [CCP § 2031.240(b)(2)].

If only part of an item or category of item in the demand is objected to, the response must include a statement of compliance, or a representation of inability to comply with respect to the remainder of that item or category [CCP § 2031.240(a)].

12.15[4] Propounding Party Should Ascertain Existence of Good Cause for Production of Electronic Evidence. The party receiving a demand for the production of electronically stored information may respond to the demand (or to a motion for a further response to the demand) by seeking a protective order on the basis that the information is from a source that is not reasonably accessible because of undue burden or expense [see CCP § 2031.060(c)].



Strategic Point:

The party seeking a protective order bears the burden of demonstrating that the information is from a source that is not reasonably accessible because of undue burden or expense [CCP § 2031.060(c)].

However, even if the information is from a source that is not reasonably accessible because of undue burden or expense, the court may nonetheless order discovery if the propounding party shows good cause for discovery [CCP § 2031.060(d)]. If the court finds good cause for the production of electronically stored information from a source that is not reasonably accessible, the court may set conditions for the discovery of the electronically stored information, including allocation of the expense of discovery [CCP § 2031.060(e)].



Cross Reference:

Protective orders, see *Ch. 11, Seeking or Opposing Protective Order, 11.03-11.12.*

Compare:

Similar procedures apply when a nonparty receives a subpoena requiring the production of electronically stored information and opposes the subpoena on the ground that the information is from a source that is

not reasonably accessible because of undue burden or expense [CCP § 1985.8(d)-(f)].

Prerequisite:

Even if the responding party does not seek a protective order on the basis that the information sought is from a source that is not reasonably accessible [see CCP § 2031.060(d)], the propounding party's motion to compel a further response must still show good cause for discovery [see CCP § 2031.310(b)(1)].

Distinguish:

Even if the source of the electronically stored information is reasonably accessible, the court must nevertheless limit the frequency or extent of discovery of that information if the court determines that (1) it is possible to obtain the information from some other source that is more convenient, less burdensome, or less expensive; (2) the discovery sought is unreasonably cumulative or duplicative; (3) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (4) the likely burden or expense of the proposed discovery outweighs the likely benefit, taking into account the amount in controversy, the resources of the parties, the importance of the issues in the litigation, and the importance of the requested discovery in resolving the issues [CCP § 2031.060(f)].

12.15[5] Propounding Party Should Ascertain Whether Responding Party Will Produce Electronic Evidence in Reasonably Usable Form. If the response to a demand for production of electronically stored information objects to the form of information specified in the demand, or if the demand does not specify a form, the responding party must specify the form in which it will produce the information [CCP § 2031.280(c); see CCP § 2031.280(d)(1)]. If the form specified by the response will not be usable by the propounding party, that party may seek a court order requiring the responding party to produce the information in a reasonably usable form [see CCP § 2031.280(d), (e)].



Strategic Point:

If the form in which the information is ordinarily maintained by the responding party will not be reasonably usable by the propounding party, any court order requiring translation of the information will probably require the propounding party to pay the expenses of translation [see CCP § 2031.280(e); see *Toshiba America Electronics Components v. Superior Court* (2004) 124 CA4th 762, 772, 21 CR2d 532]. Therefore, before making a motion for an order requiring the responding party to translate the information, the propounding party should consider simply offering to pay for the responding party to translate the information. Such an offer, if accepted, would save both parties the time and expense of a contested motion; rejection of the offer could lay the groundwork for an eventual award of sanctions if a motion becomes necessary to compel the responding party to translate the information [see CCP § 2031.310(h), (i)]. If the reasonableness of the cost and the necessity of the translation are disputed, those issues can be presented in the motion to compel a further response [see *Toshiba America Electronics Components v. Superior Court* (2004) 124 CA4th 762, 773, 21 CR2d 532].

Compare:

A party serving a subpoena requiring production of electronically stored information may specify the form in which the information is to be produced [CCP § 1985.8(b)]. Unless the subpoenaing party and the subpoenaed party otherwise agree or the court otherwise orders, if the subpoena does not specify a form for the information, the person subpoenaed must produce the information in the form in which it is ordinarily maintained or a form that is reasonably usable [CCP § 1985.8(c)(1)]. If necessary, the subpoenaed person, at the reasonable expense of the subpoenaing person, must translate the information into a reasonably usable form [CCP § 1985.8(g)].

12.15[6] Propounding Party Should Verify That Response Has Been Signed Under Oath by Appropriate Individual. If the response to a request for production has not been signed by the appropriate individual, the

propounding party may seek an order compelling the responding party to provide an appropriately signed response [see *CCP* § 2031.250]. Ordinarily, the responding party must sign the response under oath unless the response contains only objections [*CCP* § 2031.250(a)]. If the responding party is a public or private corporation or a partnership or association or governmental agency, one of its officers or agents must sign the response under oath on behalf of that party [*CCP* § 2031.250(b)].

**Trap--Responding Party:**

If the officer or agent signing the response on behalf of a party is an attorney acting in that capacity for a party, that party waives any lawyer-client privilege and any work-product protection [see *CCP* § 2018.010 et seq.] during any subsequent discovery from that attorney concerning the identity of the sources of the information contained in the response [*CCP* § 2031.250(b)].

If the response contains any objections, the attorney for the responding party must sign the response [*CCP* § 2031.250(b), (c)].

12.15[7] Counsel for Propounding Party Must Meet and Confer With Opposing Counsel Before Making Motion. Before making a motion to compel a further response, the propounding party must meet and confer with the responding party in a reasonable and good-faith attempt at an informal resolution of each issue presented by the motion [*CCP* § 2031.310(b)(2); see *CCP* § 2016.040]. The meeting and conference may be conducted in person, by telephone, or by letter [see *CCP* § 2023.010(i)].

**Warning:**

A failure to meet and confer as required constitutes a misuse of discovery, for which the court must impose a monetary sanction, regardless of the outcome of the discovery motion, ordering that the party or attorney who failed to confer as required pay the reasonable expenses (including attorney's fees) incurred by anyone as a result of that conduct [*CCP* § 2023.020].

**Cross Reference:**

Discussion of "meet-and-confer" declaration required to be filed with motion to compel further response, see 12.16[2].



58 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

IV. MOVING TO COMPEL FURTHER RESPONSE TO DEMAND FOR PRODUCTION OF ELECTRONIC EVIDENCE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.16

12.16 Counsel Must Ensure Compliance With Special Requirements for Motion.

12.16[1] Motion Must Set Forth Specific Facts Showing Good Cause for Discovery. A motion for an order compelling a further response must set forth specific facts showing good cause justifying the discovery sought by the demand [CCP § 2031.310(b)(1)].

Distinguish:

If the responding party seeks a protective order on the basis that the information sought is from a source that is not reasonably accessible because of undue burden or expense, the court may nonetheless order discovery if the propounding party shows good cause [CCP § 2031.060(d)]. The requirement that a motion to compel a further response must show good cause for discovery is an independent requirement that applies whether or not the responding party is seeking a protective order [see CCP § 2031.310(b)(1)].



Cross Reference:

Ascertaining existence of good cause for discovery, see 12.15[4].

Compare:

When a nonparty receives a subpoena requiring the production of electronically stored information and opposes the subpoena on the ground that the information is from a source that is not reasonably accessible because of undue burden or expense, the court has the power to require production of the information on a finding of good cause [CCP § 1985.8(d)-(f)].

12.16[2] Motion Must Include Meet-and-Confer Declaration. A motion to compel a further response to a demand for production of electronically stored information must include a "meet-and-confer" declaration stating facts showing a reasonable and good-faith attempt at an informal resolution of each issue presented by the motion [CCP § 2031.310(b)(2); see CCP § 2016.040].

12.16[3] Separate Statement Must Accompany Motion. A motion to compel a further response to a demand for production of electronically stored information must be accompanied by a "separate statement" [Cal Rules Ct, Rule 3.1345(a)]. A "separate statement" is a separate document filed and served with the motion that provides all the

information necessary to understand each discovery request and all the responses to it that are at issue [*Cal Rules Ct, Rule 3.1345(c)*]. The separate statement must be full and complete so that no person is required to review any other document in order to determine the full request and the full response, and material must not be incorporated into the separate statement by reference [*Cal Rules Ct, Rule 3.1345(c)*]. The separate statement must include, for each production demand to which a further response is requested, all of the following [*Cal Rules Ct, Rule 3.1345(c)*]:

- The text of the demand.
- The text of each response or objection, and any further responses.
- A statement of the factual and legal reasons for compelling further responses or production as to each matter in dispute.
- If necessary, the text of all definitions, instructions, and other matters required to understand each demand and the responses to it.
- If the response to a particular demand is dependent on the response given to another demand, or if the reasons a further response is deemed necessary are based on the response to some other demand, the other demand and the response to it must be set forth.
- If the pleadings, other documents in the file, or other items of discovery are relevant to the motion, a summary of each relevant document.

12.16[4] Motion Must Be Filed by Statutory Deadline. The propounding party must give notice of the motion to compel a further response within 45 days after service of the response, unless the parties have agreed in writing to a specific later date for giving notice [*CCP § 2031.310(c)*]. A failure to give timely notice of the motion forfeits the right to compel a further response [*CCP § 2031.310(c)*].



Warning:

The 45-day period for making the motion is measured from the date of service of the written response, not from the date of actual production [*CCP § 2031.310(c)*]; therefore, unless the parties have agreed in writing to an extended filing period, a motion to compel a further response made within 45 days of production, but more than 45 days after service of the written response, will be deemed untimely [*Sexton v. Superior Court* (1997) 58 CA4th 1403, 1409-1410, 68 CR2d 708 ; *Standon Co., Inc. v. Superior Court* (1990) 225 CA3d 898, 903, 275 CR 833] . However, even if the propounding party misses the 45-day deadline, another discovery device, such as a notice to produce documents at a deposition [see *CCP § 2025.220(a)(4)*], may be used to obtain the desired information [*Carter v. Superior Court* (1990) 218 CA3d 994, 995-996, 267 CR 290] .



59 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

IV. MOVING TO COMPEL FURTHER RESPONSE TO DEMAND FOR PRODUCTION OF ELECTRONIC EVIDENCE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.17

12.17 Movant May Address Potential Sanctions.

12.17[1] Movant May Request Sanctions Against Responding Party. The court ordinarily must impose a monetary sanction against any party, person, or attorney who unsuccessfully opposes a motion to compel a further response to a demand for production of electronically stored information [*CCP* § 2031.310(h); *see CCP* § 2023.010 *et seq.*; *see also Cal Rules Ct, Rule 3.1348(a)* (sanction may be imposed even if no formal opposition to motion was filed)].

Exceptions:

The court is not required to impose a monetary sanction if it finds that the party, person, or attorney subject to the sanction acted with substantial justification or that other circumstances make the imposition of the sanction unjust [*CCP* § 2031.310(h)]. Furthermore, absent exceptional circumstances, the court may not impose sanctions on a party or any attorney for failure to provide electronically stored information that has been lost, damaged, altered, or overwritten as a result of the routine, good-faith operation of an electronic information system [*CCP* § 2031.310(j)(1)].

Distinguish:

Only monetary sanctions may be imposed for unsuccessfully opposing an initial motion to compel a further response to a demand for production [*CCP* § 2031.310(h)]. Issue sanctions, evidence sanctions, and terminating sanctions [*see CCP* § 2023.010 *et seq.*] are available (in addition to monetary sanctions) only if the party to be sanctioned has failed to obey an order compelling a response or a further response [*CCP* §§ 2031.300(c), 2031.310(i)].

Compare:

Monetary sanctions are similarly available against a party, person, or attorney whose opposition to a motion to compel a further response includes an unsuccessful request for a protective order [*CCP* § 2031.060(h)]. In such a case, the court is not required to impose the sanction if it finds that the party, person, or attorney subject to the sanction acted with substantial justification or that other circumstances make the imposition of the sanction unjust [*CCP* § 2031.060(h)]. Furthermore, absent exceptional circumstances, the court may not impose sanctions on a party or any attorney for failure to provide electronically stored information that has been lost, damaged, altered, or overwritten as a result of the

routine, good-faith operation of an electronic information system [*CCP* § 2031.060(i)(1)].

Compare:

The court may not impose sanctions on a nonparty who fails to comply with a subpoena for the production of electronically stored information if the information has been lost, damaged, altered, or overwritten as a result of the routine, good-faith operation of an electronic information system [*CCP* § 1985.8(l)(1)].

12.17[2] Movant May Oppose Responding Party's Request for Sanctions. If the court denies the motion to compel a further response to the demand for production of electronically stored information, the court ordinarily must impose a monetary sanction on the moving party and his or her attorney [*CCP* § 2031.310(h); *see CCP* § 2023.010 *et seq.*]. The moving party may avoid sanctions, however, by establishing that the moving party (or his or her attorney) acted with substantial justification or that other circumstances make the imposition of the sanction unjust [*CCP* § 2031.310(h)].

Compare:

Monetary sanctions are similarly available against a party, person, or attorney who unsuccessfully opposes a request for a protective order [*CCP* § 2031.060(h)]. In such a case, the court is not required to impose the sanction if it finds that the party, person, or attorney subject to the sanction acted with substantial justification or that other circumstances make the imposition of the sanction unjust [*CCP* § 2031.060(h)].



60 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel
V. OPPOSING MOTION TO COMPEL FURTHER RESPONSE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.18

12.18 CHECKLIST: Opposing Motion to Compel Further Response.

- ☐ At meeting and conference requested by propounding party before motion is filed:

Authority:

CCP §§ 2031.310(b)(2), 2016.040

Discussion:

See 12.16[2]

- ☐ Determine if informal resolution can be reached on some or all issues.
- ☐ Make sure that responding party's position on any issue that remains unresolved has substantial justification, so as to avoid sanctions should court ultimately grant motion.

Authority:

CCP § 2031.310(h)

Discussion:

See 12.22[1]

- ☐ Review motion and copy of response to production demand, to determine whether to contest asserted grounds for motion, on basis of any of following:

- ☐ Each statement of compliance contained in response to demand is complete.

Authority:

CCP §§ 2031.210(a)(1), 2031.220, 2031.310(a)(1)

Discussion:

See 12.20[1]

- ☐ Any representation of inability to comply with demand is accurate and includes sufficient explanation and other required information.

Authority:

CCP §§ 2031.210(a)(2), 2031.230, 2031.310(a)(2)

Discussion:

See 12.20[2]

- ☐ Determine whether circumstances support affirmative defense to motion, such as any of following:

- ☐ Propounding party forfeited right to compel further response by failing to give notice of motion within 45 days after service of response, or later date established by parties' written agreement.

Authority:

CCP § 2031.310(c)

Discussion:

See 12.21[1]

- ☐ Information demanded is from source that is not reasonably accessible because of undue burden or expense.

Authority:

CCP § 2031.310(d)-(f)

Discussion:

See 12.21[2]

- ☐ Particular demand that is subject of motion seeks objectionable discovery.

Authority:

CCP §§ 2031.210(a)(3), 2031.240

Discussion:

See 12.21[3]

- ☐ Circumstances such as following justify court order limiting discovery:

Authority:

CCP §§ 2031.060(b), 2031.310(g)

Discussion:

See 12.21[4]

- ☐ It is possible to obtain demanded information from some other source that is more convenient, less burdensome, or less expensive.
 - ☐ Discovery sought is unreasonably cumulative or duplicative.
 - ☐ Propounding party has had ample opportunity by discovery in action to obtain information sought.
 - ☐ Likely burden or expense of proposed discovery outweighs likely benefit, taking into account amount in controversy, resources of parties, importance of issues in case, and importance of requested discovery in resolving those issues.
 - ☐ Limitation on discovery is necessary to protect responding party from unwarranted annoyance, embarrassment, or oppression, or from undue burden and expense.
- ☐ Prepare papers opposing motion.
- ☐ Prepare memorandum opposing motion, including request for monetary sanction.

Authority:

CCP § 2031.310(h); Cal Rules Ct, Rules 3.1112(a)(3), 3.1113.

Discussion:

See 12.22[2]

- ☐ Prepare affidavits or declarations, along with any appropriate exhibits, that are necessary to provide factual support for opposition.

Authority:

Cal Rules Ct, Rule 3.1112(b)

- ☐ Follow standard procedure for opposing noticed motion.

Authority:

Cal Rules Ct, Rule 3.1300 et seq.

Discussion:

See Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure, Ch. 26, Law and Motion Procedure, 26.39

- ☐ If motion is granted, demonstrate either of following:

Discussion:

See 12.22[1]

☐ That opposing party acted with substantial justification or that other circumstances make imposition of sanctions on opposing party unjust.

Authority:

CCP § 2031.310(h)

☐ That electronically stored information that was demanded has been lost, damaged, altered, or overwritten as result of routine, good-faith operation of electronic information system, and there are no exceptional circumstances justifying sanctions.

Authority:

CCP § 2031.310(j)(1)



61 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel
V. OPPOSING MOTION TO COMPEL FURTHER RESPONSE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.19

12.19 Options and Strategies.

The purpose of a motion to compel a further response is to obtain a response that completely identifies and requires the production of the available, nonprivileged documents. Once the motion is decided, there is no longer any dispute over the responding party's duty to produce the unprivileged items, and any subsequent refusal to produce those items will lead to a motion to compel compliance [*Standon Co., Inc. v. Superior Court* (1990) 225 CA3d 898, 903, 275 CR 833] . Therefore, in opposing a motion to compel a further response, counsel should vigorously and thoroughly assert any privilege, work-product protection, or trade-secret protection that might pertain to the demanded information.



62 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel
V. OPPOSING MOTION TO COMPEL FURTHER RESPONSE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.20

12.20 Responding Party May Contest Grounds for Motion.

12.20[1] Responding Party May Establish That Statement of Compliance Is Complete. If the motion to compel a further response claims that a statement of compliance in the original response is incomplete [*see CCP §§ 2031.210(a)(1), 2031.310(a)(1)*], the opposition to the motion should establish that the particular statement of compliance states that (1) the production (or the inspection, copying, testing, sampling, or related activity specified in the demand) will be allowed, either in whole or in part; and (2) all documents or things in the demanded category that are in the possession, custody, or control of the responding party and to which no objection is being made will be included in the production [*CCP § 2031.220*].

12.20[2] Responding Party May Establish Inability to Comply With Demand. If the motion to compel a further response claims that a representation of inability to comply in the original response is inadequate, incomplete, or evasive [*see CCP §§ 2031.210(a)(2), 2031.310(a)(2)*], the opposition to the motion should establish that the representation of inability to comply includes all of the following required elements [*CCP § 2031.230*]:

- An affirmation that a diligent search and a reasonable inquiry have been made in an effort to comply with that particular demand.
- A statement explaining whether the inability to comply is because the particular item or category of item never existed; has been destroyed; has been lost, misplaced, or stolen; or has never been, or is no longer, in the possession, custody, or control of the responding party.
- The name and address of any natural person or organization known or believed by the responding party to have possession, custody, or control of that particular item or category of item.



63 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel
V. OPPOSING MOTION TO COMPEL FURTHER RESPONSE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.21

12.21 Responding Party May Assert Affirmative Defenses to Motion.

12.21[1] Responding Party May Establish That Movant Forfeited Right to Compel Further Response by Waiting More Than 45 Days to Serve Motion. The propounding party's failure to give timely notice of a motion to compel a further response forfeits the right to compel a further response [*CCP § 2031.310(c)*]. To establish that a forfeiture has occurred, the opposition to the motion should show all of the following:

- The propounding party did not give notice of the motion within 45 days after service of the response to the demand.
- Either (1) the propounding and responding party did not agree in writing to any date for giving notice of the motion that was more than 45 days after service of the response to the demand; or (2) if the parties did make such an agreement, the propounding party failed to give notice of the motion on or before the agreed date [*CCP § 2031.310(c)*].

12.21[2] Responding Party May Establish That Electronic Evidence Sought by Movant Is Not Reasonably Accessible. The responding party has the burden of demonstrating that the electronically stored information demanded is from a source that is not reasonably accessible because of undue burden or expense [*CCP § 2031.310(d)*].

Consider:

A showing that the information demanded is from a source that is not reasonably accessible will not necessarily prevent discovery of the information. The court may nevertheless order discovery if the propounding party shows good cause [*CCP § 2031.310(e)*]. In such a case the court may set conditions for discovery of the information, including allocation of the expense of discovery [*CCP § 2031.310(f)*].

Compare:

Similar procedures apply when a nonparty receives a subpoena requiring the production of electronically stored information and opposes the subpoena on the ground that the information is from a source that is not reasonably accessible because of undue burden or expense [*CCP § 1985.8(d)-(f)*].

12.21[3] Responding Party May Establish Grounds for Objections to Demand. If the response to the demand for production included any objections to particular demands [*see CCP § 2031.210(a)(3)*], the opposition to the motion

to compel a further response should establish the factual basis for the objections. An objection may be based, for example, on attorney-client privilege or work-product protection [*see CCP § 2031.300(a)*; *see also CCP § 2031.285*].

Like the initial response to the demand for production, the opposition should identify with particularity the electronically stored information falling within any category of item to which an objection is made [*see CCP § 2031.240(b)(1)*]. The specific ground for, and extent of, the objection should be clearly explained [*see CCP § 2031.240(b)(2)*]. If the objection is based on a claim of privilege, the particular privilege must be identified [*see CCP § 2031.240(b)(2)*]. If an objection is based on a claim that the information sought is protected work product [*see CCP § 2018.010 et seq.*], that claim must be expressly asserted [*see CCP § 2031.240(b)(2)*].

Cross Reference:

Discussion of objection based on inaccessibility of information demanded, *see 12.21[2]*.

12.21[4] Responding Party May Establish Grounds to Limit Discovery. The court must limit the frequency or extent of discovery of electronically stored information, even from a source that is reasonably accessible, if the court determines that any of the following conditions exists [*CCP § 2031.310(g)*]:

- It is possible to obtain the information from some other source that is more convenient, less burdensome, or less expensive.
- The discovery sought is unreasonably cumulative or duplicative.
- The propounding party has had ample opportunity by discovery in the action to obtain the information sought.
- The likely burden or expense of the proposed discovery outweighs the likely benefit, taking into account the amount in controversy, the resources of the parties, the importance of the issues in the litigation, and the importance of the requested discovery in resolving the issues.

On the responding party's request, the court may make an order protecting the responding party from unwarranted annoyance, embarrassment, or oppression, or from undue burden and expense. Such an order may include any of the following directions [*CCP § 2031.060(b)*]:

- That all or some of the items or categories of items in the demand need not be produced or made available at all.
- That the time for responding to the demand, or to any particular item or category of items in the demand, be extended [*see CCP § 2031.260*].
- That the place of production be other than that specified in the demand.
- That the production be made only on specified terms and conditions.
- That a trade secret or other confidential research, development, or commercial information not be disclosed, or be disclosed only to specified persons or only in a specified way.
- That the items produced be sealed and thereafter opened only on order of the court.

Compare:

The court has similar powers to limit the frequency or extent of discovery, and to protect against undue

burden or expense, when a nonparty has been subpoenaed to produce electronically stored information [CCP § 1985.8(h), (k)].



64 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel
V. OPPOSING MOTION TO COMPEL FURTHER RESPONSE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.22

12.22 Responding Party May Address Potential Sanctions.

12.22[1] Responding Party May Oppose Movant's Request for Sanctions. If the court grants the motion to compel a further response to the demand for production, the court ordinarily must impose a monetary sanction on the opposing party and his or her attorney [CCP § 2031.310(h); see CCP § 2023.010 et seq.; see also Cal Rules Ct, Rule 3.1348(a) (sanction may be imposed even if no formal opposition to motion was filed)]. However, the opposing party may avoid sanctions by establishing any of the following:

- The opposing party (or his or her attorney) acted with substantial justification [CCP § 2031.310(h)].
- Other circumstances make the imposition of the sanction unjust [CCP § 2031.310(h)].

Example:

A responding party that revealed the existence of documents, sought a confidentiality agreement, and successfully moved for a protective order was justified, as a matter of law, in opposing a motion to compel production of those documents while the motion for a protective order was pending. The court of appeal, therefore, reversed a sanctions order against the responding party [*Foothill Props. v. Lyon/Copley Corona Assocs. (1996) 46 CA4th 1542, 1557-1558, 54 CR2d 488*] .

- The electronically stored information that was demanded has been lost, damaged, altered, or overwritten as a result of the routine, good-faith operation of an electronic information system, and there are no exceptional circumstances justifying sanctions [CCP § 2031.310(j)(1)].



Strategic Point:

Only monetary sanctions may be imposed for unsuccessfully opposing an initial motion to compel a further response to a demand for production [CCP § 2031.310(h)]. Issue sanctions, evidence sanctions, and terminating sanctions [see CCP § 2023.010 et seq.] are available (in addition to monetary sanctions) only if the party to be sanctioned has failed to obey an order compelling a response or a further response [CCP §§ 2031.300(c),

2031.310(i)].

Compare:

Monetary sanctions are similarly available, with similar limitations, against a party, person, or attorney whose opposition to a motion to compel a further response includes an unsuccessful request for a protective order [*CCP* § 2031.060(h), (i)(1)].

Compare:

The court may not impose sanctions on a nonparty who fails to comply with a subpoena for the production of electronically stored information if the information has been lost, damaged, altered, or overwritten as a result of the routine, good-faith operation of an electronic information system [*CCP* § 1985.8(l)(1)].

12.22[2] Responding Party May Request Sanctions Against Unsuccessful Movant. If the court denies the motion to compel a further response to a demand for production of electronically stored information, the court ordinarily must impose a monetary sanction [*see CCP* § 2023.010 *et seq.*] against the moving party and the moving party's attorney [*CCP* § 2031.310(h)].

Exception:

The court is not required to impose a monetary sanction if it finds that the party, person, or attorney subject to the sanction acted with substantial justification or that other circumstances make the imposition of the sanction unjust [*CCP* § 2031.310(h)].

Compare:

Monetary sanctions are similarly available against a party, person, or attorney who unsuccessfully opposes a request for a protective order [*CCP* § 2031.060(h)]. In such a case, the court is not required to impose the sanction if it finds that the party, person, or attorney subject to the sanction acted with substantial justification or that other circumstances make the imposition of the sanction unjust [*CCP* § 2031.060(h)].



65 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

VI. MOVING TO COMPEL COMPLIANCE WITH STATEMENT OF COMPLIANCE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.23

12.23 CHECKLIST: Moving to Compel Compliance With Statement of Compliance.

- ☐ Verify that responding party has failed to produce electronically stored information in accordance with statement of compliance contained in response to demand, as supplemented by statutory requirements and any agreement between parties.

Authority:

CCP §§ 2031.210(a)(1), 2031.220, 2031.280, 2031.320(a)

Discussion:

See 12.25

- ☐ Consider meeting and conferring with opposing counsel to attempt to resolve issues informally, even though "meet and confer" declaration is not required for motion to compel compliance with statement of compliance.

Authority:

CCP § 2031.320(a)

Discussion:

See 12.24

- ☐ Prepare necessary documents for motion to compel further response.
- ☐ Prepare notice of motion and motion to compel compliance with statement of compliance, including request for monetary sanctions.

Authority:

CCP § 2031.320(a); Cal Rules Ct, Rules 3.1110, 3.1112(a)

Discussion:

See 12.27[1]

Form:

See 12.39

- ☐ Prepare memorandum in support of motion.

Authority:

Cal Rules Ct, Rules 3.1112(a)(3), 3.1113

- ☐ Prepare affidavits or declarations, along with any appropriate exhibits, that are necessary to provide factual support for motion.

Authority:

Cal Rules Ct, Rule 3.1112(b)

- ☐ Prepare "separate statement" providing all information necessary to understand each demand and all responses to it that are at issue.

Authority:

Cal Rules Ct, Rule 3.1345(a), (c)

Discussion:

See 12.26

- ☐ Prepare proposed order.

Authority:

Cal Rules Ct, Rule 3.1112(b)

Form:

See 12.41

- ☐ Follow standard procedure for noticed motion.

Authority:

Cal Rules Ct, Rule 3.1300 et seq.

Discussion:

Standard motion procedure, see *Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure*, Ch. 26, *Law and Motion Procedure*, 26.39

- ☐ If motion is denied, demonstrate that moving party acted with substantial justification or that other circumstances make imposition of sanctions on moving party unjust.

Authority:

CCP § 2031.320(b)

Discussion:

See 12.27[2]



66 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

VI. MOVING TO COMPEL COMPLIANCE WITH STATEMENT OF COMPLIANCE

*1-12 MB Practice Guide: CA E-Discovery and Evidence 12.24***12.24 Options and Strategies.**

If the responding party fails to produce the demanded electronically stored information in accordance with that party's statement of compliance [see CCP §§ 2031.210(a)(1), 2031.220], the propounding party may move for an order compelling compliance with the statement of compliance (also called a motion to compel compliance with the demand for production or a motion to compel compliance with the response) [CCP § 2031.320(a)].

Distinguish--Motion to Compel Further Response:

The purpose of a motion to compel compliance is simply to require that the responding party produce the demanded items in accordance with the response served by that party and accepted by the propounding party. Any dispute over the response, including any disputed claim of privilege, should be resolved through a motion to compel a further response brought within 45 days of the service of the response [*Standon Co., Inc. v. Superior Court* (1990) 225 CA3d 898, 903, 275 CR 833 ; see CCP § 2031.310(a), (c)]. A motion to compel compliance is not subject to the 45-day deadline that applies to a motion to compel a further response [*Standon Co., Inc. v. Superior Court* (1990) 225 CA3d 898, 903, 275 CR 833 ; compare CCP § 2031.320(a) with CCP § 2031.310(c)]. However, a motion to compel compliance is subject to the generally applicable requirement that all discovery motions be heard on or before the 15th day before the date initially set for trial CCP § 2024.020(a)]; that generally applicable cutoff for the hearing of discovery motions can be extended by agreement of the parties, or by the court in its case management order or in response to a party's motion [see CCP §§ 2024.050, 2024.060; *Cal Rules Ct, Rule 3.728*; see also *Cal Rules Ct, Rules 3.724, 3.727*].

**Cross Reference:**

Discussion of motion to compel further response, see 12.13-12.17.

The moving papers for a motion to compel compliance include a motion and notice of motion, one or more declarations establishing the factual basis for the motion, a "separate statement" of information describing the discovery requests and responses at issue, and a memorandum in support of the motion [*Cal Rules of Ct, Rules 3.1112(a), (b), 3.1345(a)*].

**Strategic Point--Reasonable Diligence:**

Unlike a motion to compel a further response, a motion to compel compliance need not be preceded by

an attempt to settle the matter informally, and no "meet and confer" declaration need accompany the motion [*compare CCP § 2031.320(a) with CCP § 2031.310(b)(2); see also CCP § 2016.040*]. However, counsel should nevertheless attempt to contact opposing counsel to determine if the failure to comply with the statement of compliance was an oversight that can be remedied quickly and cost-effectively without a formal motion. Even if the matter is not resolved informally, offering opposing counsel the opportunity to rectify the failure to respond can lay the groundwork for an award of sanctions if a motion becomes necessary to obtain a response [*see CCP § 2031.320(b)*].

**Cross Reference:**

Discussion of sanctions, see 12.27[1].



67 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

VI. MOVING TO COMPEL COMPLIANCE WITH STATEMENT OF COMPLIANCE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.25

12.25 Movant Must Establish That Responding Party Has Failed to Produce Electronic Evidence in Accordance With Statement of Compliance.

If the responding party fails to produce the demanded electronically stored information in accordance with that party's statement of compliance [*see CCP §§ 2031.210(a)(1), 2031.220*], the propounding party may move for an order compelling compliance [*CCP § 2031.320(a)*].

Generally, production of the demanded information under a statement of compliance is subject to the following requirements:

- Any electronically stored information produced in response to the demand must either be produced as it is kept in the usual course of business, or be organized and labeled to correspond with the categories in the demand [*CCP § 2031.280(a)*].
- The information must be produced on the date specified in the demand [*see CCP § 2031.030(c)(2)*], unless an objection has been made to that date. If the date for inspection has been extended by agreement of the parties [*see CCP § 2031.270*], the information must be produced on the agreed date [*CCP § 2031.280(b)*].
- If the responding party objects to a specified form for producing the electronically stored information, or if no form is specified in the demand, the responding party must produce the information in the form specified in the statement of compliance [*CCP § 2031.280(c)*]. If the demand did not specify a form, then unless the parties otherwise agree or the court otherwise orders, 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)(1)*]. The responding party need not produce the information in more than one form [*CCP § 2031.280(d)(2)*].



Strategic Point:

If the responding party balks at the cost of translating the information into a reasonably usable form, the propounding party should consider offering to pay the reasonable cost of translation, as that is what the court will probably order anyway [*see CCP § 2031.280(e)*; *see also Toshiba America Electronics Components v. Superior Court* (2004) 124 CA4th 762, 772, 21 CR2d 532]. Similarly, a party

subpoenaing a nonparty to produce electronically stored information may be required to pay the reasonable expense translating the information into a reasonably usable form [*CCP* § 1985.8(*g*)].



68 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

VI. MOVING TO COMPEL COMPLIANCE WITH STATEMENT OF COMPLIANCE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.26

12.26 Counsel Must Prepare Separate Statement to Accompany Motion.

A motion to compel compliance with a statement of compliance must be accompanied by the "separate statement" that is required whenever a motion involves the content of a discovery request or a response to a discovery request [*Cal Rules Ct, Rule 3.1345(a), (c)*].

➡ **Cross Reference:**

Discussion of Separate Statement, see 12.16[3].



69 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

VI. MOVING TO COMPEL COMPLIANCE WITH STATEMENT OF COMPLIANCE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.27

12.27 Movant May Address Potential Sanctions.

12.27[1] Movant May Request Sanctions Against Responding Party. The court ordinarily must impose a monetary sanction against any party, person, or attorney who unsuccessfully opposes a motion to compel compliance with a demand for production of electronically stored information [*CCP* § 2031.320(b); see *CCP* § 2023.010 et seq.; see also *Cal Rules Ct*, Rule 3.1348(a) (sanction may be imposed even if no formal opposition to motion was filed)].

Exceptions:

- The court is not required to impose a monetary sanction if it finds that the party, person, or attorney subject to the sanction acted with substantial justification or that other circumstances make the imposition of the sanction unjust [*CCP* § 2031.320(b)].
- Absent exceptional circumstances, the court may not impose sanctions on a party or any attorney for failure to provide electronically stored information that has been lost, damaged, altered, or overwritten as a result of the routine, good-faith operation of an electronic information system [*CCP* § 2031.320(d)(1)].

Distinguish:

Only monetary sanctions may be imposed for unsuccessfully opposing an initial motion to compel compliance with a demand for production [*CCP* § 2031.320(b)]. Issue sanctions, evidence sanctions, and terminating sanctions [see *CCP* § 2023.010 et seq.] are available (in addition to monetary sanctions) only if the party to be sanctioned has failed to obey an order compelling a response to, a further response to, or compliance with, a demand [*CCP* §§ 2031.300(c), 2031.310(i), 2031.320(c)].

Compare:

Monetary sanctions are similarly available against a party, person, or attorney whose opposition to a motion to compel compliance with a statement of compliance includes an unsuccessful request for a protective order [*CCP* § 2031.060(h)]. In such a case, the court is not required to impose the sanction if it finds that the party, person, or attorney subject to the sanction acted with substantial justification or that other circumstances make the imposition of the sanction unjust [*CCP* § 2031.060(h)]. Furthermore, absent exceptional circumstances, the court may not impose sanctions on a party or any attorney for

failure to provide electronically stored information that has been lost, damaged, altered, or overwritten as a result of the routine, good-faith operation of an electronic information system [CCP § 2031.060(i)(1)].

Compare:

The court may not impose sanctions on a nonparty who fails to comply with a subpoena for the production of electronically stored information if the information has been lost, damaged, altered, or overwritten as a result of the routine, good-faith operation of an electronic information system [CCP § 1985.8(l)(1)].

12.27[2] Movant May Oppose Responding Party's Request for Sanctions. If the court denies the motion to compel compliance with the demand, the court ordinarily must impose a monetary sanction against the moving party and his or her attorney [CCP § 2031.320(b); see CCP § 2023.010 *et seq.*]. However, the moving party may avoid sanctions by establishing that the moving party (or his or her attorney) acted with substantial justification or that other circumstances make the imposition of the sanction unjust [CCP § 2031.320(b)].

Compare:

Monetary sanctions are similarly available against a party, person, or attorney who unsuccessfully opposes a request for a protective order [CCP § 2031.060(h)]. In such a case, the court is not required to impose the sanction if it finds that the party, person, or attorney subject to the sanction acted with substantial justification or that other circumstances make the imposition of the sanction unjust [CCP § 2031.060(h)].



70 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

VII. OPPOSING MOTION TO COMPEL COMPLIANCE WITH STATEMENT OF COMPLIANCE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.28

12.28 CHECKLIST: Opposing Motion to Compel Compliance With Statement of Compliance.

- ☐ Review specific allegations in motion, copy of response to production demand, and documentation of actual production of information, to determine whether motion may be opposed on basis of factual disputes pertaining to matters such as time, format, and cost of production.

Authority:

CCP §§ 2031.270, 2031.280

Discussion:

See 12.30

- ☐ Prepare papers opposing motion.

- ☐ Prepare memorandum opposing motion, including request for monetary sanction.

Authority:

CCP § 2031.320(b); Cal Rules Ct, Rules 3.1112(a)(3), 3.1113

Discussion:

See 12.31[2]

- ☐ Prepare affidavits or declarations, along with any appropriate exhibits, that are necessary to provide factual support for opposition.

Authority:

Cal Rules Ct, Rules 3.1112(b)

- ☐ Follow standard procedure for opposing noticed motion.

Authority:

Cal Rules Ct, Rule 3.1300 et seq.

Discussion:

See Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure, Ch. 26, Law and Motion Procedure, 26.46

☐ If motion is granted, demonstrate either of following:

Discussion:

See 12.31[1]

☐ That opposing party acted with substantial justification or that other circumstances make imposition of sanctions on opposing party unjust.

Authority:

CCP § 2031.320(b)

☐ That electronically stored information that was demanded has been lost, damaged, altered, or overwritten as result of routine, good-faith operation of electronic information system, and there are no exceptional circumstances justifying sanctions.

Authority:

CCP § 2031.310(d)(1)



71 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

VII. OPPOSING MOTION TO COMPEL COMPLIANCE WITH STATEMENT OF COMPLIANCE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.29

12.29 Options and Strategies.

The purpose of a motion to compel compliance is simply to require that the responding party produce the demanded items in accordance with the response served by that party and accepted by the propounding party [*see CCP § 2031.320(a)*].

Any dispute over an objection or claim of privilege asserted by the responding party in the response to the demand should have been resolved through a motion to compel a further response brought within 45 days of the service of the response [*Standon Co., Inc. v. Superior Court* (1990) 225 CA3d 898, 903, 275 CR 833 ; *see CCP § 2031.310(a), (c)*]. Accordingly, the main basis for opposing a motion to compel compliance will be factual: the responding party will simply demonstrate that the actual production matches what was promised in the response. The court will not consider any attempt by the propounding party to contest an objection or claim of privilege that survived an earlier motion to compel a further response (or that survived the 45-day period for making a motion compel a further response) [*see Standon Co., Inc. v. Superior Court* (1990) 225 CA3d 898, 903, 275 CR 833] .



Cross Reference:

Discussion of opposition to motion to compel further response, see *12.18-12.22*.



72 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

VII. OPPOSING MOTION TO COMPEL COMPLIANCE WITH STATEMENT OF COMPLIANCE

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.30

12.30 Responding Party Should Establish That Electronic Evidence Has Been Produced in Accordance With Statement of Compliance.

A motion for an order compelling compliance with a statement of compliance [*see CCP § 2031.320(a); see also CCP §§ 2031.210(a)(1), 2031.220*] may be opposed on factual grounds. Depending on the specific allegations of noncompliance set forth in the motion, the opposing party may need to present factual evidence establishing one or more of the following:

- The electronically stored information produced in response to the demand was produced as it is kept in the usual course of business, or it was organized and labeled to correspond with the categories in the demand [*see CCP § 2031.280(a)*].
- The information was produced on the date specified in the demand [*see CCP § 2031.030(c)(2)*] or on a later date agreed to in writing by the parties [*see CCP §§ 2031.270, 2031.280(b)*].
- The electronically stored information was produced either (1) in the form specified in the demand, or (2) if no form was specified in the demand, the information was produced in a reasonably usable form specified in the statement of compliance or in a form agreed to by the parties or ordered by the court [*CCP § 2031.280(c), (d)(1)*].
- Compliance is not possible because the electronically stored information that was demanded has been lost, damaged, altered, or overwritten as a result of the routine, good-faith operation of an electronic information system [*CCP § 2031.320(d)(1)*].
- The propounding party refused to bear the burden, imposed on the propounding party by statute, of paying the cost of translating the information into a reasonably usable form [*see CCP § 2031.280(e)*].

Compare:

Similarly, a party subpoenaing a nonparty to produce electronically stored information may be required to pay the reasonable expense translating the information into a reasonably usable form [*CCP § 1985.8(g)*].



73 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel

VII. OPPOSING MOTION TO COMPEL COMPLIANCE WITH STATEMENT OF COMPLIANCE

*1-12 MB Practice Guide: CA E-Discovery and Evidence 12.31***12.31 Responding Party May Address Potential Sanctions.**

12.31[1] Responding Party May Oppose Movant's Request for Sanctions. If the court grants the motion to compel compliance with a demand for production of electronically stored information, the court ordinarily must impose a monetary sanction on the opposing party and his or her attorney [*CCP* § 2031.320(b); see *CCP* § 2023.010 et seq.; see also *Cal Rules Ct*, Rule 3.1348(a) (sanction may be imposed even if no formal opposition to motion was filed)]. However, the opposing party may avoid sanctions by establishing any of the following:

- The opposing party (or his or her attorney) acted with substantial justification [*CCP* § 2031.320(b)].
- Other circumstances make the imposition of the sanction unjust [*CCP* § 2031.320(b)].
- The electronically stored information that was demanded has been lost, damaged, altered, or overwritten as a result of the routine, good-faith operation of an electronic information system, and there are no exceptional circumstances justifying sanctions [*CCP* § 2031.320(d)(1)].

Strategic Point:

If the propounding party seeks issue sanctions, evidence sanctions, or terminating sanctions [see *CCP* § 2023.010 et seq.], counsel should point out to the court that such sanctions may not be imposed for unsuccessfully opposing an initial motion to compel compliance with the demand for production [*CCP* § 2031.320(b)]. Those sanctions are available only if the party to be sanctioned has failed to obey an order compelling a response to, a further response to, or compliance with, a demand [*CCP* §§ 2031.300(c), 2031.310(i), 2031.320(c)].

Compare:

Monetary sanctions are similarly available against a party, person, or attorney whose opposition to a motion to compel compliance with a statement of compliance includes an unsuccessful request for a protective order [*CCP* § 2031.060(h)]. In such a case, the court is not required to impose the sanction if it finds that the party, person, or attorney subject to the sanction acted with substantial justification or that other circumstances make the imposition of the sanction unjust [*CCP* § 2031.060(h)]. In addition, absent

exceptional circumstances, the court may not impose sanctions on a party or any attorney for failure to provide electronically stored information that has been lost, damaged, altered, or overwritten as a result of the routine, good-faith operation of an electronic information system [CCP § 2031.060(i)(1)].

Compare:

The court may not impose sanctions on a nonparty who fails to comply with a subpoena for the production of electronically stored information if the information has been lost, damaged, altered, or overwritten as a result of the routine, good-faith operation of an electronic information system [CCP § 1985.8(l)(1)].

12.31[2] Responding Party May Request Sanctions Against Unsuccessful Movant. The court ordinarily must impose a monetary sanction [see CCP § 2023.010 *et seq.*] against any party, person, or attorney who unsuccessfully makes a motion to compel compliance with a demand for production of electronically stored information [CCP § 2031.320(b)].

Exception:

The court is not required to impose a monetary sanction if it finds that the party, person, or attorney subject to the sanction acted with substantial justification or that other circumstances make the imposition of the sanction unjust [CCP § 2031.320(b)].

Compare:

Monetary sanctions are similarly available against a party, person, or attorney who unsuccessfully opposes a request for a protective order [CCP § 2031.060(h)]. In such a case, the court is not required to impose the sanction if it finds that the party, person, or attorney subject to the sanction acted with substantial justification or that other circumstances make the imposition of the sanction unjust [CCP § 2031.060(h)].



74 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel
VIII. FORMS

*1-12 MB Practice Guide: CA E-Discovery and Evidence 12.32***12.32 Notice of Motion and Motion to Compel Response to Demand for Production of Electronic Evidence.**

Notice of Motion and Motion to Compel Response to Demand for Production of Electronic Evidence.

Tom Doe

California Bar Number 987654

100 North Main St., Suite 200

Farallon City, California 90000

Phone: 555-555-5555

Attorney for Plaintiff, John Smith

SUPERIOR COURT OF CALIFORNIA,

COUNTY OF FARALLON

John Smith, Plaintiff, vs. Mary Jones Enterprises,
Inc., Defendant.

)
) No. _____
) NOTICE OF MOTION AND MOTION
) TO COMPEL RESPONSE TO DEMAND
) FOR PRODUCTION OF
) ELECTRONICALLY STORED INFORMATION
) Date: _____
) Time: _____
) Location: _____
) Judge: _____
) Date Action Filed: _____
) Trial Date: _____
)

To Defendant, Mary Jones Enterprises, Inc., and its attorney of record:

NOTICE IS HEREBY GIVEN that, on _____ [date], at _____ [time], or as soon
thereafter as the matter may be heard, in [_____ (Department or Division) _____ of]
this court, located at 1 North Main Street, Farallon City, California, Plaintiff, John Smith, will, and hereby does, move

for an order compelling Defendant to respond to _____ [e.g., Plaintiff's Demand for Production of Electronically Stored Information, Set #1], declaring that Defendant has waived any objections to discovery of the information sought in the Demand, and awarding sanctions against Defendant.

The motion is based on this notice of motion, the accompanying declaration of _____ [name], the accompanying supporting memorandum, the records and file herein, and such evidence as may be presented at the hearing on the motion.

Dated: _____

Respectfully submitted,

_____ [signature]

Tom Doe

Attorney for Plaintiff, John Smith

NOTES:

Authority:

CCP § 2031.300; Cal Rules Ct, Rule 3.1112(a)

Checklist:

See 12.03

Discussion:

See 12.05-12.07

Related Form for Declaration Supporting Motion:

See 12.33

Related Form for Order:

See 12.35



75 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel
VIII. FORMS*1-12 MB Practice Guide: CA E-Discovery and Evidence 12.33***12.33 Declaration Supporting Motion to Compel Response to Demand for Production of Electronic Evidence.**

Declaration Supporting Motion to Compel Response to Demand for Production of Electronic Evidence.

Tom Doe

California Bar Number 987654

100 North Main St., Suite 200

Farallon City, California 90000

Phone: 555-555-5555

Attorney for Plaintiff, John Smith

SUPERIOR COURT OF CALIFORNIA,

COUNTY OF FARALLON

John Smith, Plaintiff, vs. Mary Jones Enterprises,
Inc., Defendant.

)
) No. _____
) DECLARATION OF _____ [e.g.,
) TOM DOE] IN SUPPORT OF
) MOTION TO COMPEL
) RESPONSE TO
) DEMAND FOR
) PRODUCTION OF
) ELECTRONICALLY
) STORED INFORMATION
) Date: _____
) Time: _____
) Location: _____
) Judge: _____
) Date Action Filed: _____
) Trial Date: _____

I, _____ [e.g., Tom Doe], declare:

1. I am _____ [e.g., an attorney at law duly admitted to practice before all the courts of the State of California and the attorney of record herein for Plaintiff John Smith].
2. The subject matter of this action is _____ [state nature of action].
3. On _____ [date], _____ [propounding party, e.g., Plaintiff John Smith] served _____ [responding party, e.g., Defendant Mary Jones Enterprises, Inc.,] with _____ [identify demand, e.g., Plaintiff's Demand for Production of Electronically Stored Information, Set #1,] for the purpose of _____ [specify, e.g., inspecting and copying the records of all electronic communications between Plaintiff and Defendant regarding the agreement at issue]. A true and correct copy of this Demand is attached as Exhibit A and incorporated by reference.
4. A response to _____ [identify demand, e.g., Plaintiff's Demand for Production of Electronically Stored Information, Set #1,] was due on _____ [date].
5. To date, _____ [responding party, e.g., Defendant Mary Jones Enterprises, Inc.,] has failed to serve a response.
6. _____ [Moving party, e.g., Plaintiff John Smith] bases his/her request for the imposition of a sanction in the amount of \$_____ on _____ [itemize and explain, in as many paragraphs as necessary, the basis of the computation of the monetary amount of sanction requested].

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Dated: _____

_____ [signature]

[typed name]

NOTES:

Authority:

CCP § 2031.300; Cal Rules Ct, Rule 3.1112(b)

Checklist:

See 12.03

Discussion:

See 12.05, 12.07

Related Form for Motion and Notice of Motion:

See 12.32

Related Form for Order:

See 12.35



76 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel
VIII. FORMS

*1-12 MB Practice Guide: CA E-Discovery and Evidence 12.34***12.34 Declaration Opposing Motion to Compel Response to Demand for Production of Electronic Evidence.**

Declaration Opposing Motion to Compel Response to Demand for Production of Electronic Evidence.

Jane Lee

California Bar Number 123456

50 South Main St., Suite 100

Farallon City, California 90000

Phone: 555-999-9999

Attorney for Defendant, Mary Jones Enterprises, Inc.

SUPERIOR COURT OF CALIFORNIA,

COUNTY OF FARALLON

	)	
	)	No. _____
	)	DECLARATION OF
	)	_____ [e.g., MARY JONES] OP-
John Smith, Plaintiff, vs. Mary Jones Enterprises,	)	POSING
Inc., Defendant.	)	MOTION TO COMPEL
	)	RESPONSE TO
	)	DEMAND FOR
	)	PRODUCTION OF
	)	ELECTRONICALLY
	)	STORED INFORMATION

I, _____ [name of declarant, e.g., Jane Lee], declare:

1. I am _____ [e.g., an attorney at law duly admitted to practice before all the courts of the State of California and the attorney of record herein for Defendant Mary Jones Enterprises, Inc.]

2. On _____ [date], _____ [propounding party, e.g., Plaintiff John Smith] served _____ [responding party, e.g., Defendant Mary Jones Enterprises, Inc.,] with _____ [

identify demand, e.g., Plaintiff's Demand for Production of Electronically Stored Information, Set #1].

[Set forth basis for opposing motion, e.g.:]

3. _____ *[Responding party, e.g., Defendant]* subsequently served a response to the Demand on _____ *[date]*, a date set by written agreement of the parties. A true and correct copy of that agreement is attached to this Declaration.

[OR:]

3. The failure of _____ *[responding party, e.g., Defendant Mary Jones Enterprises, Inc.,]* to serve a timely response to the Demand was the result of _____ *[mistake or inadvertence or excusable neglect]* in that _____ *[specify, e.g., the Demand was delivered by the postal service to the wrong office and was not received by Defendant's counsel until October 15, 2010, the day after the response was due]* .

4. _____ *[Responding party, e.g., Defendant]* subsequently served a response that was in substantial compliance with *Code of Civil Procedure Sections 2031.210, 2031.220, 2031.230, 2031.240, and 2031.280* on October 29, 2010.

[CONTINUE]

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Dated: _____

_____ *[signature]*

[typed name]

NOTES:

Authority:

CCP § 2031.300; Cal Rules Ct, Rule 3.1112(b)

Checklist:

See 12.03

Discussion:

See 12.05, 12.07

Related Form for Motion and Notice of Motion:

See 12.32

Related Form for Order:

See 12.35



77 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel
VIII. FORMS

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.35

12.35 Order Compelling Response to Demand for Production of Electronic Evidence.

Order Compelling Response to Demand for Production of Electronic Evidence.
SUPERIOR COURT OF CALIFORNIA,
COUNTY OF FARALLON

	)	
	)	No. _____
John Smith, Plaintiff, vs. Mary Jones Enterprises,	)	ORDER--RESPONSE TO DEMAND FOR
Inc., Defendant.	)	PRODUCTION OF ELECTRONICALLY
	)	STORED EVIDENCE
	)	

The motion of _____ [*moving party, e.g., Plaintiff John Smith*] to compel _____ [*opposing party, e.g., Defendant Mary Jones Enterprises, Inc.,*] to respond to _____ [*e.g., Plaintiff's Demand for Production of Electronically Stored Information, Set #1,*] came on regularly for hearing by the Court on _____ [*date*]. Plaintiff appeared by counsel Tom Doe; Defendant appeared by counsel Jane Lee.

The Court, having considered the declarations and other documents in support of and in opposition to the motion, having heard the arguments of counsel, and being fully advised in the matter, finds as follows: _____ [*opposing party, e.g., Defendant Mary Jones Enterprises, Inc.,*] failed to serve a timely response to _____ [*e.g., Plaintiff's Demand for Production of Electronically Stored Information, Set #1,*], and the failure to file a timely response was not the result of mistake, inadvertence, or excusable neglect.

IT IS THEREFORE ORDERED that the motion be, and hereby is, granted, and that _____ [*party from whom production is sought, e.g., Defendant Mary Jones Enterprises, Inc.,*] serve a full and complete response, without raising any objections, to _____ [*e.g., Plaintiff's Demand for Production of Electronically Stored Information, Set #1,*] on or before _____ [*date*].

[*If imposing sanctions:*]

IT IS FURTHER ORDERED that _____ [*specify unsuccessful party and attorney, e.g., Defendant Mary Jones Enterprises, Inc., and its attorney Jane Lee*] pay forthwith to _____ [*specify successful party, e.g., Plaintiff John Smith*] the sum of \$_____ as reasonable expenses and attorney's fees.

[*OR, if not ordering sanctions:*]

On further proof made to the satisfaction of the court that _____ [*specify unsuccessful party and attorney, e.g., Defendant Mary Jones Enterprises, Inc., and its attorney Jane Lee*] _____ [*acted with substantial justification or specify other circumstances making imposition of a sanction unjust*], IT IS FURTHER ORDERED that no monetary sanction be imposed on [*specify unsuccessful party and attorney, e.g., Defendant Mary Jones Enterprises, Inc., or its attorney Jane Lee*].

[*CONTINUE*]

Dated: _____
_____ [*signature*]
Judge of the Superior Court

NOTES:

Authority:

CCP § 2031.300

Checklist:

See 12.03

Discussion:

See 12.05-12.07

Related Form for Motion and Notice of Motion:

See 12.32

Related Declarations:

See 12.33, 12.34



78 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel
VIII. FORMS

1-12 MB Practice Guide: CA E-Discovery and Evidence 12.36

12.36 Notice of Motion and Motion to Compel Further Response to Demand for Production of Electronic Evidence.

Notice of Motion and Motion to Compel Further Response to Demand for Production of Electronic Evidence.

Tom Doe

California Bar Number 987654

100 North Main St., Suite 200

Farallon City, California 90000

Phone: 555-555-5555

Attorney for Plaintiff, John Smith

SUPERIOR COURT OF CALIFORNIA,

COUNTY OF FARALLON

John Smith, Plaintiff, vs. Mary Jones Enterprises,
Inc., Defendant.

)
) No. _____
) NOTICE OF MOTION
) AND MOTION
) TO COMPEL
) FURTHER RESPONSE
) TO DEMAND FOR
) PRODUCTION OF
) ELECTRONICALLY
) STORED INFORMATION
) Date: _____
) Time: _____
) Location: _____
) Judge: _____
) Date Action Filed: _____
) Trial Date: _____
)

To Defendant, Mary Jones Enterprises, Inc., and its attorney of record:

NOTICE IS HEREBY GIVEN that, on _____ [date], at _____ [time], or as soon thereafter as the matter may be heard, in [_____ (Department or Division) _____ of] this court, located at 1 North Main Street, Farallon City, California, Plaintiff, John Smith, will, and hereby does, move for an order compelling Defendant to serve a further response to _____ [e.g., Plaintiff's Demand for Production of Electronically Stored Information, Set #1,] and awarding sanctions against Defendant.

The motion is made on the grounds that _____ [e.g., Defendant's initial statement of compliance as to Item 5 of the Demand is incomplete in that it does not specify whether Defendant will produce all documents in the demanded category that are within the Defendant's possession or Defendant's initial representation of inability to comply with Item 7 of the Demand is incomplete in that it does not affirm that a diligent search and a reasonable inquiry have been made in an effort to comply with that Demand or Defendant's objection to the relevance of Item 9 of the Demand is without merit] . There is good cause for the discovery sought by the Demand, because _____ [state specific facts showing good cause].

The motion is based on this notice of motion, the accompanying declaration of _____ [name], the accompanying separate statement submitted pursuant *California Rules of Court, Rule 3.1345(a)*, the accompanying supporting memorandum, the records and file herein, and such evidence as may be presented at the hearing on the motion.

Dated: _____

Respectfully submitted,

_____ [signature]

Tom Doe

Attorney for Plaintiff, John Smith

NOTES:

Authority:

CCP § 2031.310; Cal Rules Ct, Rule 3.1112(a)

Checklist:

See 12.13

Discussion:

See 12.15-12.17

Related Form for Declaration Supporting Motion:

See 12.37

Related Form for Order:

See 12.38



79 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel
VIII. FORMS

*1-12 MB Practice Guide: CA E-Discovery and Evidence 12.37***12.37 Declaration Supporting Motion to Compel Further Response to Demand for Production of Electronic Evidence.**

Declaration Supporting Motion to Compel Further Response to Demand for Production of Electronic Evidence.
Tom Doe

California Bar Number 987654

100 North Main St., Suite 200

Farallon City, California 90000

Phone: 555-555-5555

Attorney for Plaintiff, John Smith

SUPERIOR COURT OF CALIFORNIA,

COUNTY OF FARALLON

John Smith, Plaintiff, vs. Mary Jones Enterprises,
Inc., Defendant.

)
) No. _____
) DECLARATION OF _____ [e.g.,
) TOM DOE] IN SUPPORT OF
) MOTION TO COMPEL
) FURTHER RESPONSE
) TO DEMAND FOR
) PRODUCTION OF
) ELECTRONICALLY
) STORED INFORMATION
) Date: _____
) Time: _____
) Location: _____
) Judge: _____
) Date Action Filed: _____
) Trial Date: _____

I, _____ [e.g., Tom Doe], declare:

1. I am _____ [*e.g.*, an attorney at law duly admitted to practice before all the courts of the State of California and the attorney of record herein for Plaintiff John Smith].
2. The subject matter of this action is _____ [*state nature of action*].
3. On _____ [*date*], _____ [*propounding party, e.g.*, Plaintiff John Smith] served _____ [*responding party, e.g.*, Defendant Mary Jones Enterprises, Inc.,] with _____ [*identify demand, e.g.*, Plaintiff's Demand for Production of Electronically Stored Information, Set #1,] for the purpose of _____ [*specify, e.g.*, inspecting and copying the records of all electronic communications between Plaintiff and Defendant regarding the agreement at issue]. A true and correct copy of this Demand is attached as Exhibit A and incorporated by reference.
4. Good cause exists justifying the discovery sought by _____ [*identify demand, e.g.*, Plaintiff's Demand for Production of Electronically Stored Information, Set #1,] because _____ [*e.g.*, the electronic communications are relevant to establish the meaning of certain provisions of the agreement at issue].
5. On _____ [*date*], _____ [*responding party, e.g.*, Defendant Mary Jones Enterprises, Inc.,] served a response to the Demand.
6. The response served by _____ [*responding party, e.g.*, Defendant Mary Jones Enterprises, Inc.,] is inadequate in that _____ [*e.g.*, Defendant's statement of compliance as to Item 5 of the Demand is incomplete in that it does not specify whether Defendant will produce all documents in the demanded category that are within the Defendant's possession or Defendant's representation of inability to comply with Item 7 of the Demand is incomplete in that it does not affirm that a diligent search and a reasonable inquiry have been made in an effort to comply with that Demand or Defendant's objection to the relevance of Item 9 of the Demand is without merit].
7. _____ [*State facts showing reasonable, good-faith attempt to arrive at informal resolution of issues presented in motion, e.g.*, On November 19, 2011, I met with Jane Lee, Defendant's counsel, in an attempt to resolve the issues described in Paragraph 6, above, but we were unable to resolve the matter].
8. _____ [*Moving party, e.g.*, Plaintiff John Smith] bases his/her request for the imposition of a sanction in the amount of \$_____ on _____ [*itemize and explain, in as many paragraphs as necessary, the basis of the computation of the monetary amount of sanction requested*].

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Dated: _____

_____ [*signature*]

[*typed name*]

NOTES:

Authority:

CCP §§ 2016.040, 2031.310; Cal Rules Ct, Rule 3.1112(b)

Checklist:

See 12.13

Discussion:

See *12.15-12.17*

Related Form for Motion and Notice of Motion:

See *12.36*

Related Form for Order:

See *12.38*



80 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel
VIII. FORMS

*1-12 MB Practice Guide: CA E-Discovery and Evidence 12.38***12.38 Order Compelling Further Response to Demand for Production of Electronic Evidence.**

Order Compelling Further Response to Demand for Production of Electronic Evidence.
SUPERIOR COURT OF CALIFORNIA,
COUNTY OF FARALLON

John Smith, Plaintiff, vs. Mary Jones Enterprises,
Inc., Defendant.

)
)
) No. ____
) ORDER--FURTHER RESPONSE TO
) DEMAND FOR PRODUCTION OF
) ELECTRONICALLY STORED EVIDENCE
)

The motion of _____ [*moving party, e.g., Plaintiff John Smith*] to compel _____
[*opposing party, e.g., Defendant Mary Jones Enterprises, Inc.,*] to further respond to _____ [*e.g.,*
Plaintiff's Demand for Production of Electronically Stored Information, Set #1,] came on regularly for hearing by the
Court on _____ [*date*]. Plaintiff appeared by counsel Tom Doe; Defendant appeared by counsel Jane
Lee.

The Court, having considered the declarations and other documents in support of and in opposition to the motion,
having heard the arguments of counsel, and being fully advised in the matter, finds as follows: _____
[*e.g., Defendant's initial statement of compliance as to Item 5 of the Demand is incomplete in that it does not specify
whether Defendant will produce all documents in the demanded category that are within the Defendant's possession or
Defendant's initial representation of inability to comply with Item 7 of the Demand is incomplete in that it does not
affirm that a diligent search and a reasonable inquiry have been made in an effort to comply with that Demand or
Defendant's objection to the relevance of Item 9 of the Demand is without merit*]. The Court further finds that there is
good cause for discovery of these items.

IT IS THEREFORE ORDERED that the motion be, and hereby is, granted, and that _____ [*party from
whom production is sought, e.g., Defendant Mary Jones Enterprises, Inc.,*] serve a further, complete response, without
raising any objections, to _____ [*e.g., Items 5, 7, and 9 of Plaintiff's Demand for Production of*

Electronically Stored Information, Set #1,) on or before _____ [date].

[If imposing sanctions:]

IT IS FURTHER ORDERED that _____ [specify unsuccessful party and attorney, e.g., Defendant Mary Jones Enterprises, Inc., and its attorney Jane Lee] pay forthwith to _____ [specify successful party, e.g., Plaintiff John Smith] the sum of \$_____ as reasonable expenses and attorney's fees.

[OR, if not ordering sanctions:]

On further proof made to the satisfaction of the court that _____ [specify unsuccessful party and attorney, e.g., Defendant Mary Jones Enterprises, Inc., and its attorney Jane Lee] _____ [acted with substantial justification or specify other circumstances making imposition of a sanction unjust], IT IS FURTHER ORDERED that no monetary sanction be imposed on [specify unsuccessful party and attorney, e.g., Defendant Mary Jones Enterprises, Inc., or its attorney Jane Lee].

[CONTINUE]

Dated: _____
_____ [signature]

Judge of the Superior Court

NOTES:

Authority:

CCP § 2031.310

Checklist:

See 12.13

Discussion:

See 12.15-12.17

Related Form for Motion and Notice of Motion:

See 12.36

Related Declaration:

See 12.37



81 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel
VIII. FORMS

*1-12 MB Practice Guide: CA E-Discovery and Evidence 12.39***12.39 Notice of Motion and Motion to Compel Compliance With Statement of Compliance.**

Order Compelling Further Response to Demand for Production of Electronic Evidence.

Tom Doe

California Bar Number 987654

100 North Main St., Suite 200

Farallon City, California 90000

Phone: 555-555-5555

Attorney for Plaintiff, John Smith

SUPERIOR COURT OF CALIFORNIA,

COUNTY OF FARALLON

John Smith, Plaintiff, vs. Mary Jones Enterprises,
Inc., Defendant.

)
) No. _____
) NOTICE OF MOTION AND MOTION
) TO COMPEL COMPLIANCE WITH
) DEMAND FOR PRODUCTION OF
) ELECTRONICALLY STORED INFORMATION
) Date: _____
) Time: _____
) Location: _____
) Judge: _____
) Date Action Filed: _____
) Trial Date: _____
)

To Defendant, Mary Jones Enterprises, Inc., and its attorney of record:

NOTICE IS HEREBY GIVEN that, on _____ [date], at _____ [time], or as soon
thereafter as the matter may be heard, in [_____ (Department or Division) _____ of]
this court, located at 1 North Main Street, Farallon City, California, Plaintiff, John Smith, will, and hereby does, move

for an order compelling Defendant to comply with Defendant's response to _____ [e.g., Plaintiff's Demand for Production of Electronically Stored Information, Set #1,] and awarding sanctions against Defendant.

The motion is made on the ground that _____ [e.g., Defendant has refused to produce its electronically stored records of e-mail correspondence between the parties sent or received in March 2010, as required by Item 3 of the Demand, even though Defendant's initial response included a statement of compliance with Item 3].

The motion is based on this notice of motion, the accompanying declaration of _____ [name], the accompanying separate statement submitted pursuant *California Rules of Court, Rule 3.1345(a)*, the accompanying supporting memorandum, the records and file herein, and such evidence as may be presented at the hearing on the motion.

Dated: _____

Respectfully submitted,

_____ [signature]

Tom Doe
Attorney for Plaintiff, John Smith

NOTES:

Authority:

CCP § 2031.320; Cal Rules Ct, Rule 3.1112(a)

Checklist:

See 12.23

Discussion:

See 12.25-12.27

Related Form for Declaration Supporting Motion:

See 12.40

Related Form for Order:

See 12.41



82 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel
VIII. FORMS*1-12 MB Practice Guide: CA E-Discovery and Evidence 12.40***12.40 Declaration Supporting Motion to Compel Compliance With Statement of Compliance.**

Declaration Supporting Motion to Compel Compliance With Statement of Compliance.

Tom Doe

California Bar Number 987654

100 North Main St., Suite 200

Farallon City, California 90000

Phone: 555-555-5555

Attorney for Plaintiff, John Smith

SUPERIOR COURT OF CALIFORNIA,

COUNTY OF FARALLON

John Smith, Plaintiff, vs. Mary Jones Enterprises,
Inc., Defendant.

)
) No. _____
) DECLARATION OF _____ [e.g.,
) TOM DOE] IN SUPPORT OF
) MOTION TO COMPEL
) COMPLIANCE WITH
) DEMAND FOR
) PRODUCTION OF
) ELECTRONICALLY
) STORED INFORMATION
) Date: _____
) Time: _____
) Location: _____
) Judge: _____
) Date Action Filed: _____
) Trial Date: _____

I, _____ [e.g., Tom Doe], declare:

1. I am _____ [e.g., an attorney at law duly admitted to practice before all the courts of the State of California and the attorney of record herein for Plaintiff John Smith].
2. The subject matter of this action is _____ [state nature of action].
3. On _____ [date], _____ [pounding party, e.g., Plaintiff John Smith] served _____ [responding party, e.g., Defendant Mary Jones Enterprises, Inc.,] with _____ [identify demand, e.g., Plaintiff's Demand for Production of Electronically Stored Information, Set #1,] for the purpose of _____ [specify, e.g., inspecting and copying the records of all electronic communications between Plaintiff and Defendant regarding the agreement at issue]. A true and correct copy of this Demand is attached as Exhibit A and incorporated by reference.
4. On _____ [date], _____ [responding party, e.g., Defendant Mary Jones Enterprises, Inc.,] served a response to the Demand.
5. The response served by _____ [responding party, e.g., Defendant Mary Jones Enterprises, Inc.,] included a statement that defendant would comply with Item 3 of the Demand, which asked for Defendant's electronically stored records of e-mail correspondence between the parties sent or received in March 2010].
6. To date, _____ [responding party, e.g., Defendant Mary Jones Enterprises, Inc.,] has refused to comply with that response.
7. _____ [Moving party, e.g., Plaintiff John Smith] bases his/her request for the imposition of a sanction in the amount of \$ _____ on _____ [itemize and explain, in as many paragraphs as necessary, the basis of the computation of the monetary amount of sanction requested].

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Dated: _____

_____ [signature]

[typed name]

NOTES:

Authority:

CCP § 2031.320; Cal Rules Ct, Rule 3.1112(b)

Checklist:

See 12.23

Discussion:

See 12.25-12.27

Related Form for Motion and Notice of Motion:

See 12.39

Related Form for Order:

See 12.41



83 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 12 Obtaining or Opposing Motion to Compel
VIII. FORMS

*1-12 MB Practice Guide: CA E-Discovery and Evidence 12.41***12.41 Order Compelling Compliance With Statement of Compliance.**

Order Compelling Compliance With Statement of Compliance.
SUPERIOR COURT OF CALIFORNIA,
COUNTY OF FARALLON

	)	
	)	No. _____
John Smith, Plaintiff, vs. Mary Jones Enterprises,	)	ORDER--COMPLIANCE WITH DEMAND
Inc., Defendant.	)	FOR PRODUCTION OF ELECTRONICALLY
	)	STORED EVIDENCE
	)	

The motion of _____ [*moving party, e.g., Plaintiff John Smith*] to compel _____ [*opposing party, e.g., Defendant Mary Jones Enterprises, Inc.,*] to comply with _____ [*e.g., Plaintiff's Demand for Production of Electronically Stored Information, Set #1,*] came on regularly for hearing by the Court on _____ [*date*]. Plaintiff appeared by counsel Tom Doe; Defendant appeared by counsel Jane Lee.

On proof made to the Court's satisfaction, and good cause appearing:

IT IS ORDERED that the motion be, and hereby is, granted and that _____ [*party from whom production is sought, e.g., Defendant Mary Jones Enterprises, Inc.,*] produce at _____ [*time*], on _____ [*date*], at _____ [*specify place, e.g., the law offices of Tom Doe, located at 100 North Main St., Suite 200, Farallon City, California,*] the following:

_____ [*Designate each category for which production is ordered, and set forth terms and conditions relating to the manner in which inspection or related activities will be conducted, as well as any other terms and conditions prescribed by court*].

[*If imposing sanctions:*]

IT IS FURTHER ORDERED that _____ [*specify unsuccessful party and attorney, e.g., Defendant Mary Jones Enterprises, Inc., and its attorney Jane Lee*] pay forthwith to _____ [*specify successful party, e.g., Plaintiff John Smith*] the sum of \$_____ as reasonable expenses and attorney's fees.

[*OR, if not ordering sanctions:*]

On further proof made to the satisfaction of the court that _____ [*specify unsuccessful party and attorney, e.g., Defendant Mary Jones Enterprises, Inc., and its attorney Jane Lee*] _____ [*acted with substantial justification or specify other circumstances making imposition of a sanction unjust*], IT IS FURTHER ORDERED that no monetary sanction be imposed on [*specify unsuccessful party and attorney, e.g., Defendant Mary Jones Enterprises, Inc., or its attorney Jane Lee*].

[*CONTINUE*]

Dated: _____
_____ [*signature*]
Judge of the Superior Court

NOTES:

Authority:

CCP § 2031.320

Checklist:

See 12.23

Discussion:

See 12.25-12.27

Related Form for Motion and Notice of Motion:

See 12.39

Related Declaration:

See 12.40



84 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 13 Seeking or Opposing Sanctions for Noncompliance

1-13 MB Practice Guide: CA E-Discovery and Evidence 13.syn

§ 13.syn Synopsis to Chapter 13: Seeking or Opposing Sanctions for Noncompliance

13.01 Scope.

13.02 Objective and Strategy.

13.03 CHECKLIST: Determining Whether Grounds for Sanctions Exist.

13.04 Spoliation of ESI Is Sanctionable.

13.04[1] Parties Have a Duty to Preserve Evidence.

13.04[2] Scope of Duty to Preserve.

13.04[3] When Duty to Preserve ESI Arises.

13.04[4] Litigant's Duty to Preserve Can Extend to ESI Held by Third Parties.

13.05 Destruction of ESI May Be Intentional or Negligent.

13.05[1] Intentional Destruction in Anticipation of or in Response to Discovery Request Is a Misuse of Discovery Process.

13.05[2] Negligent Destruction May Be Sanctionable.

13.06 Sanctions Against Third-Party Spoliators Are Limited.

13.07 Safe Harbor Protects Good Faith Loss of ESI.

13.08 Types of Sanctions for Spoliation.

13.08[1] Monetary Sanction.

13.08[2] Issue Sanction.

13.08[3] Evidence Sanction.

13.08[4] Adverse Inference.

13.08[5] Terminating Sanction.

13.08[6] Contempt Sanction.

13.08[7] An Attorney May Be Disciplined for Spoliation.

13.08[8] Criminal Penalties Are Available for Willful Spoliation.

13.09 A Party May Be Sanctioned for Disobeying a Discovery Order or Unsuccessfully Making or Opposing a Motion to Compel.

13.09[1] Unsuccessful Party in Motion to Compel Response to Inspection Demand Is Subject to Mandatory Monetary Sanction.

13.09[2] Party That Disobeys Order Compelling Response Is Subject to Issue, Evidence, or Terminating Sanction and Monetary Sanction.

13.09[3] Unsuccessful Party in Motion to Compel Further Response to Inspection Demand Is Subject to Mandatory Monetary Sanction.

13.09[4] Party That Disobeys Order Compelling Further Response Is Subject to Issue, Evidence, or Terminating Sanction and Monetary Sanction.

13.09[5] Unsuccessful Party in Motion to Compel Compliance With Inspection Demand Is Subject to Mandatory Monetary Sanction.

13.09[6] Party That Disobeys Order Compelling Inspection Is Subject to Issue, Evidence, or Terminating Sanction and Monetary Sanction.

13.10 Failure to Return Inadvertently Disclosed Privileged Information Can Result in Disqualification of Counsel.

13.11 CHECKLIST: Procedure for Seeking Sanctions.

13.12 Motion for Order Imposing Issue, Evidence, or Terminating Sanction and Monetary Sanction.

13.12[1] Moving Papers.

13.12[1][a] Notice of Motion.

13.12[1][b] Notice of Motion Must Be Supported by Memorandum.

13.12[1][c] Notice of Motion Must Be Accompanied by Declaration If Monetary Sanction Is Sought.

13.12[1][d] Notice of Motion for Issue or Evidence Sanction Must Be Accompanied by Separate Statement.

13.12[1][e] Default Judgment Requires Supporting Evidence.

13.12[2] Order.

13.12[2][a] Losing Party Should Request Written Findings.

13.12[2][b] Written Findings Are Required When Mandatory Monetary Sanctions Are Not Imposed.

13.12[2][c] Imposition of Monetary Sanctions Against Attorney Requires Finding.

13.13 Order to Show Cause for Contempt.

13.13[1] Affidavit Required for Indirect Contempt.

13.13[2] Notice or Order to Show Cause Required.

13.13[3] Personal Service and Full Hearing Required.

13.13[4] Judgment of Contempt.

13.13[4][a] Judgment Must Specify Act and Include Finding That Act Is Within Contemner's Power.

13.13[4][b] Judgment Should Contain Factual Findings.

13.14 CHECKLIST: Opposing Imposition of Sanctions.

13.15 Options and Strategies for Opposing Imposition of Sanctions.

13.15[1] Opposing Imposition of Monetary Sanction.

13.15[1][a] Showing Substantial Justification to Render Mandatory Imposition of Monetary Sanction Unjust.

13.15[1][b] Limiting Amount of Sanction to Reasonable Expenses.

13.15[1][c] Opposing Sanction Against Attorney on Ground That Attorney Did Not Advise Conduct.

13.15[1][d] Opposing Imposition of Attorney's Fees Incurred by Pro Se Litigant.

13.15[2] Opposing Imposition of Issue, Evidence, or Terminating Sanction.

13.15[2][a] Issue, Evidence, and Terminating Sanctions Are Serious Sanctions, Not to Be Considered Lightly.

13.15[2][b] Less Drastic Alternatives May Be Appropriate.

13.15[3] Opposing Imposition of Sanction for Misuse of Discovery Process on Ground of Improper Notice or Absence of Opportunity for Hearing.

13.15[3][a] Party Opposing Sanction May Object to Notice and Absence of Opportunity to Be Heard.

13.15[3][b] Party Opposing Sanction May Object to Noncompliance With Statutory Motion Requirements.

13.15[4] Opposing Contempt Sanction.

13.15[4][a] Person Cannot Be Punished for Indirect Contempt in Absence of Personal Service and Full Hearing for Indirect Contempt.

13.15[4][b] Person Cannot Be Punished for Indirect Contempt in Absence of Sufficient Affidavit.

13.15[4][c] Contempt Sanction for Discovery Enforcement Is Drastic.

13.15[4][d] Person Is Not Subject to Contempt for Failing to Perform Act That He or She Is Incapable of Performing.

13.15[4][e] Affidavit in Opposition Should Set Forth Facts Explaining Circumstances.

13.16 -13.19 [Reserved]

13.20 Notice of Motion, Motion, and Supporting Declaration for Imposition of Issue, Evidence, or Terminating Sanction, and Monetary Sanctions Based on Discovery Misuse.

13.21 Separate Statement Supporting Motion for Issue or Evidence Sanction.

13.22 Order on Motion for Imposition of Issue, Evidence or Terminating Sanction, and Monetary Sanction.

13.23 Order to Show Cause Re Contempt and Supporting Declaration.



85 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 13 Seeking or Opposing Sanctions for Noncompliance

I. STRATEGY

1-13 MB Practice Guide: CA E-Discovery and Evidence 13.01

13.01 Scope.

This chapter covers sanctions for noncompliance in e-discovery matters, specifically:

- Objectives and strategies regarding sanctions in e-discovery matters [see 13.02].
- Duty to preserve evidence [see 13.04].
- Spoliation of evidence [see 13.05].
- Types of sanctions for spoliation of evidence [see 13.08].
- Sanctions for disobeying a discovery order or unsuccessfully making or opposing a motion to compel [see 13.09].
- Disqualification of counsel for failure to return inadvertently disclosed privileged information [see 13.10].
- Motion for order imposing sanctions [see 13.12].
- Order to show cause for contempt [see 13.13].
- Strategies for opposing sanctions [see 13.15].
- Obtaining relief from dismissal or default sanction [see 13.16-13.18].

Core Statutes:

CCP §§ 1211, 2023.010, 2023.030, 2023.040, 2031.300-2031.320; Cal Rule of Court, Rule 3.1345



86 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 13 Seeking or Opposing Sanctions for Noncompliance
I. STRATEGY

*1-13 MB Practice Guide: CA E-Discovery and Evidence 13.02***13.02 Objective and Strategy.**

As in other areas of the law, sanctions relating to electronic discovery are available to correct or deter misconduct by a party or its attorneys. Both intentional and unintentional conduct may be sanctioned.

The loss or destruction of electronic evidence ("spoliation") is a common sanctions issue. Sanctions obviously may be warranted when a party intentionally deletes e-mails or wipes a hard drive to avoid producing electronically stored information in response to a pending inspection demand. In other cases, a party's misconduct may be not as blatant, but still potentially sanctionable, as when a company fails to instruct some employees to suspend its ordinary document retention policy in order to preserve data.

Because destruction of evidence may constitute a misuse of discovery in violation of *CCP* §§ 2023.010 and 2023.030, it subjects the offending party to a wide range of potential sanctions, ranging from monetary sanctions to terminating sanctions. In addition, a lawyer who receives inadvertently produced material and fails to notify the sender can face disqualification.

Strategic Points:

Counsel for all parties should keep the following in mind:

- E-discovery sanctions can win the case when conduct is egregious.
- There may be a series of discovery motions and increasing sanctions [*see, e.g., Zubulake v. UBS Warburg LLC (SDNY 2003) 220 FRD 212, 218*] because sometimes getting additional discovery as a result of the first successful motion to compel will reveal additional misconduct that will be the subject of another motion.
- A well-planned and documented discovery effort will make sanctions easier to get--counsel should make sure that the opponent is on notice that ESI is demanded and must be preserved.

**Cross References:**

General coverage of the imposition of sanctions in the context of discovery, see Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 3, Sanctions.

General coverage of sanctions in pretrial litigation, see Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure, Ch. 35, Sanctions.

Detailed coverage of sanctions in the context of civil litigation, see California Forms of Pleading and Practice, Ch. 510, Sanctions (Matthew Bender).

Points and authorities relating to sanctions, see California Points and Authorities, Ch. 207, Sanctions (Matthew Bender).



87 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 13 Seeking or Opposing Sanctions for Noncompliance
II. DETERMINING WHETHER GROUNDS FOR SANCTIONS EXIST

1-13 MB Practice Guide: CA E-Discovery and Evidence 13.03

13.03 CHECKLIST: Determining Whether Grounds for Sanctions Exist.

☐ Has a party deleted or destroyed electronically stored evidence pursuant to a routine document destruction policy after the party reasonably anticipated litigation?

Authority:

CCP § 2023.030; Keithley v. Home Store.com, Inc. (ND Cal 2008) 2008 US Dist LEXIS 61741 ; Zubulake v. UBS Warburg LLC (SDNY 2003) 220 FRD 212, 218

Discussion:

See 13.04

Forms:

See 13.20-13.22

☐ Has a party altered or destroyed electronically stored evidence *in anticipation of* a discovery request?

Authority:

CCP § 2023.030; Cedars-Sinai Med. Ctr. v. Superior Court (1998) 18 C4th 1, 12

Discussion:

See 13.05

Forms:

See 13.20-13.22

☐ Has a party altered or destroyed electronically stored evidence *in response to* a discovery request?

Authority:

CCP § 2023.030; Cedars-Sinai Med. Ctr. v. Superior Court (1998) 18 C4th 1, 12

Discussion:

See 13.05

Forms:

See 13.20-13.22

- ☐ Has a third party suppressed or destroyed electronically stored evidence?

Authority:

Temple Cmty. Hosp. v. Superior Court (1999) 20 C4th 464, 477, 84 CR2d 852, 976 P2d 223

Discussion:

See 13.06

Forms:

See 13.20, 13.22-13.23

- ☐ Has a party unsuccessfully made or opposed a motion to compel the production of electronically stored evidence?

☐ Has a party unsuccessfully made or opposed a motion to compel a response to an inspection demand?

Authority:

CCP § 2031.300(c)

Discussion:

See 13.09[1]

- ☐ Has a party unsuccessfully made or opposed a motion to compel further response to an inspection demand?

Authority:

CCP § 2031.310(d)

Discussion:

See 13.09[3]

- ☐ Has a party unsuccessfully made or opposed a motion compelling inspection?

Authority:

CCP § 2031.320(b)

Discussion:

See 13.09[5]

- ☐ Has a party disobeyed a discovery order?

- ☐ Has a party disobeyed an order compelling a response to an inspection demand?

Authority:

CCP § 2031.300(c)

Discussion:

See 13.09[2]

- ☐ Has a party disobeyed an order compelling further response to an inspection demand?

Authority:

CCP § 2031.310(e)

Discussion:

See 13.09[4]

- ☐ Has a party disobeyed an order compelling inspection?

Authority:

CCP § 2031.320(c)

Discussion:

See 13.09[6]

- ☐ Has a party misused inadvertently produced privileged information?

Authority:

Rico v. Mitsubishi Motors Corp. (2007) 42 C4th 807, 817 ; State Comp. Ins. Fund v. WPS, Inc. (1999) 70 CA4th 644, 656-657

Discussion:

See 13.10

- ☐ Which sanctions are available?

☐ Monetary sanction.

☐ Issue sanction.

☐ Evidence sanction.

☐ Adverse inference.

☐ Terminating sanction.

☐ Contempt sanction.

☐ Attorney discipline.

☐ Criminal penalties.

Authority:

CCP § 2023.030; Evid Code §§ 412-413; B&P Code § 6106; Pen Code § 135; Cal Rules Prof Conduct, Rules 3-210, 5-200, 5-220; Cedars-Sinai Med. Ctr. v. Superior Court (1998) 18 C4th 1, 11

Discussion:

See 13.08



88 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 13 Seeking or Opposing Sanctions for Noncompliance
II. DETERMINING WHETHER GROUNDS FOR SANCTIONS EXIST

1-13 MB Practice Guide: CA E-Discovery and Evidence 13.04

13.04 Spoliation of ESI Is Sanctionable.

13.04[1] Parties Have a Duty to Preserve Evidence. Destroying evidence in anticipation of a discovery request or in response to a discovery request constitutes a misuse of discovery in violation of *CCP §§ 2023.010 and 2023.030* [*Cedars-Sinai Med. Ctr. v. Superior Court* (1998) 18 C4th 1, 12, 74 CR2d 248, 954 P2d 511 ; *R.S. Creative, Inc. v. Creative Cotton, Ltd.* (1999) 75 CA4th 486, 495, 89 CR2d 353 (affirming order resulting in terminating sanctions for forging contract and destroying evidence by use of computers in violation of stipulation not to use the computers pending examination by expert)].

13.04[2] Scope of Duty to Preserve. The California e-discovery rules do not specifically address the scope of the duty to preserve. Commentators have suggested that it is likely the duty to preserve will be interpreted to be broader than the duty to produce, and have counseled caution in matters regarding the scope of document preservation under California law [see Kiesel & Williams, *California's 2009 E-Discovery Laws--Text and Analysis* (LexisNexis 2009), § 4[5]].

In federal courts, the scope of the duty to preserve has been described as extending to what the party knows, or reasonably should know [*Keithley v. Home Store.com, Inc.* (ND Cal 2008) 2008 US Dist LEXIS 61741] :

- Is relevant in the action;
- Is reasonably calculated to lead to the discovery of admissible evidence;
- Is reasonably likely to be requested during discovery; and/or
- Is the subject of a pending discovery request.

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 [*Zubulake v. UBS Warburg LLC* (SDNY 2003) 220 FRD 212, 218 ; see *UMG Recordings, Inc. v. Hummer Winblad Venture Partners (In re Napster, Inc. Copyright Litig.)* (ND Cal 2006) 462 F Supp2d 1060, 1070 (imposing sanctions against defendant for failing to stop its policy of deleting e-mails once the duty to preserve attached)]. The duty to preserve extends to those employees likely to have relevant information--the "key players" in the case [*Zubulake v. UBS Warburg LLC* (SDNY 2003) 220 FRD

212, 218] .

Examples--Insufficient Document Preservation:

- Although the defendant circulated two document hold memoranda to certain employees, many other employees never received the memoranda, and the defendant failed to remind employees of the need to continue to preserve relevant documents and electronically stored information. In addition, the defendant could not show that e-mails were saved when computers were replaced and did not ensure that an outside IT contractor observed the litigation hold. As a result, the defendant was able to produce e-mail files for only 13 out of 57 current and former employees who were the "key players" in the case. The court imposed adverse inference and monetary sanctions [*Gordon Partners, et. al. v. Blumenthal (In re NTL, Inc. Sec. Litig.) (SDNY 2007) 244 FRD 179, 198*] .

- A federal district court imposed sanctions on defendants who lacked a written document retention and litigation hold policy and could not produce even a single e-mail notice to relevant employees [*Keithley v. Home Store.com, Inc. (ND Cal 2008) 2008 US Dist LEXIS 61741 at*18*] .



Warning:

The client's litigation hold instructions should be put in writing and communicated to all employees who might be considered "key players" in actual or anticipated litigation. Make sure that the client maintains written evidence of the steps it takes to preserve evidence.

13.04[3] When Duty to Preserve ESI Arises. Under California law, the precise point at which the duty to preserve documents comes into existence is not yet clear. Commentators have suggested that it is likely that California case law may develop along lines similar to federal law [see Kiesel & Williams, California's 2009 E-Discovery Laws--Text and Analysis (LexisNexis 2009), § 4[3]]. The California Supreme Court, in discussing spoliation of evidence, has stated that "[d]estroying evidence in response to a discovery request *after litigation has commenced* would surely be a misuse of discovery within the meaning of [CCP §] 2023" and therefore sanctionable [*Cedars-Sinai Med. Ctr. v. Superior Court* (1998) 18 Cal. 4th 1, 12, 74 CR2d 248, 954 P2d 511 (emphasis added)]. However, the decision did not deal with the question of the earliest point at which the duty to preserve evidence could initially arise.

Under federal common law, the duty to preserve documents attaches when a party should have known that the evidence may be relevant to future litigation [*Zubulake v. UBS Warburg LLC (SDNY 2003) 220 FRD 212, 216*] . The future litigation must be "probable," that is, more than a possibility [*Hynix Semiconductor Inc. v. Rambus, Inc. (ND Cal 2006) 2006 US Dist LEXIS 30690, *57*] .

Examples:

- In a patent infringement case, defendants' duty to preserve evidence did not arise from a letter from plaintiffs regarding licensing, because that letter did not threaten litigation or mention infringement. However, the duty to preserve certainly arose when plaintiffs sent defendants a letter stating that they assumed that defendant wished to litigate this matter, and threatening to "advance this matter accordingly unless we hear otherwise" by a given deadline [*Keithley v. Home Store.com, Inc. (ND Cal 2008) 2008 US Dist LEXIS 61741, *16*] .

- Duty to preserve evidence by suspending document retention policy requiring routine automated destruction of e-mails older than 90 days was not triggered by correspondence and telephone conversations; although plaintiff's communications expressed discontent, they did not threaten litigation,

and plaintiff waited nearly two years to file an action [*Cache La Poudre Feeds, LLC v. Land O'Lakes Farmland Feed, LLC* (D Colo 2007) 244 FRD 614, 623] .

- Plaintiff's president telephoned defendant's president and said he believed defendant's company (a competitor) was using plaintiff's software. The two companies had previously been involved in litigation. Defendant's president immediately ordered his employees to delete from defendant's computers all software the president had not purchased for the company or did not own. Plaintiff filed suit a month later, and sent an evidence preservation letter three weeks after filing suit. Defendant continued to delete and overwrite e-mails and other electronic evidence after receiving the letter. The court held that plaintiff was entitled to an adverse inference instruction to the jury at trial as a sanction for the spoliation [*KCH Services, Inc. v. Vanaire, Inc.* (WD Ky 2009) 2009 US Dist LEXIS 62993] .



Strategic Points:

- When drafting a pre-litigation demand letter, include a demand that the putative opponent preserve all potentially relevant materials, including electronically stored information [see, e.g., *Lombardo v. Broadway Stores*, 2002 Cal. App. Unpub. LEXIS 4700, 1-2 (Cal. App. 4th Dist. 2002) (noting that letters demanding preservation of evidence were ignored)].

- Once litigation has begun, unless the court orders another time period, counsel are required to meet and confer at least 30 days before the date set for the initial case management conference regarding any issues related to the preservation of discoverable electronically stored information [Cal Rules Ct, Rule 3.724(8)].



Cross References:

Discussion of meet and confer requirements regarding electronically stored information, see *Ch. 5, 5.14-5.21*.

Discussion of preservation of electronically stored information, see *Ch. 5, 5.03-5.08*.

13.04[4] Litigant's Duty to Preserve Can Extend to ESI Held by Third Parties. The Electronic Discovery Act authorizes a party to obtain discovery of "electronically stored information in the possession, custody, or control of any other party to the action" [CCP § 2031.010(a)]. Although there have been no reported California cases interpreting when electronically stored information held by a third party is in the "possession, custody, or control" of a litigant, federal cases interpreting the same phrase "possession, custody, or control" in Fed. Rule *Civil Proc. 34(a)(1)* provide guidance. Under federal law, a litigant has "control" over documents held by a third party--and thus a duty to preserve those documents--if the litigant has the, "right, authority, or practical ability to obtain the documents from a non-party to the action." [*Gordon Partners, et. al. v. Blumenthal (In re NTL, Inc. Sec. Litig.)* (SDNY 2007) 244 FRD 179, 195] .

Examples:

- A company that was a defendant in securities litigation entered into bankruptcy and two main companies emerged from the bankruptcy reorganization. One of the companies was a successor in liability to the original company and became a defendant in the securities litigation. The other company was not. The district court relied on a document-sharing clause in the de-merger agreement between the two companies to hold that the successor had a duty to ensure that the other company preserved

documents relevant to the securities litigation. The court granted the plaintiff's request for an adverse inference spoliation instruction sanction [*Gordon Partners, et. al. v. Blumenthal (In re NTL, Inc. Sec. Litig.) (SDNY 2007) 244 FRD 179, 195*] .

■ A company sued by a consultant for breach of a project agreement did not have "control" over electronically stored information prepared or maintained by another consultant who had participated in the project. There was no agreement between the company and the second consultant that would have given the company access to his documents. Therefore, the plaintiff was not entitled to discovery sanctions for the company's failure to ask the second consultant to preserve evidence relating to the project, although the plaintiff was entitled to sanctions for other spoliation by the company [*Goodman v. Praxair Services (D Md 2009) 632 F Supp2d 494, 515-516*] .

■ A janitorial service working at an airport had knowledge of airport procedures for reporting accidents, the existence of a recording system to capture radio communications, and the existence of the surveillance video system used at the airport. Under these circumstances, the janitorial service had a duty to take steps to ensure that the airport preserved and did not recycle videotapes of a slip-and-fall incident. A janitorial service employee "had knowledge of the accident and the apparent seriousness of [p]laintiff's injury as well, which should have put a reasonable company providing janitorial services on notice of potential liability arising from a slip and fall" [*Jain v. Memphis Shelby County Airport Auth. (WD Tenn Feb. 25, 2010) 2010 U.S. Dist. LEXIS 16842, *11*] . The court granted plaintiff's request for a sanction consisting of a permissive jury instruction that they were allowed, but not required, to presume that the missing videotape would have been unfavorable to the defendants [*Jain v. Memphis Shelby County Airport Auth., 2010 U.S. Dist. LEXIS 16842, *15*] .



89 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 13 Seeking or Opposing Sanctions for Noncompliance
II. DETERMINING WHETHER GROUNDS FOR SANCTIONS EXIST

1-13 MB Practice Guide: CA E-Discovery and Evidence 13.05

13.05 Destruction of ESI May Be Intentional or Negligent.

13.05[1] Intentional Destruction in Anticipation of or in Response to Discovery Request Is a Misuse of Discovery Process. Destroying electronically stored evidence in response to a discovery request after litigation has commenced is a misuse of discovery within the meaning of *CCP § 2023.030*, as is destruction in anticipation of a discovery request [see *Cedars-Sinai Med. Ctr. v. Superior Court* (1998) 18 C4th 1, 12, 74 CR2d 248, 954 P2d 511 (rejecting tort cause of action for first-party intentional spoliation of evidence in favor of existing remedies (citing former *CCP § 2023(a)(4), (6), (b)* (now *CCP §§ 2023.010, 2023.030*))].

Examples:

- The court granted a terminating sanction, striking defendants' cross-complaints and answer and ordering defendants' default entered, after defendants repeatedly failed to comply with discovery orders and intentionally destroyed electronically stored evidence requested by plaintiffs by running a program to erase e-mails from computer hard drives [*Electronic Funds Solutions, LLC v. Murphy* (2005) 134 CA4th 1161, 1183-1184, 36 CR3d 663] .

- In an unpublished decision, a California appellate court affirmed a monetary sanction of \$90,000 against defendant executive in a breach of fiduciary case brought by her former employer. During discovery, plaintiff demanded access to company-issued laptop computers still in the executive's possession. The executive then installed and ran a "scrubbing" program prior to handing over the computers. Plaintiff's forensic expert was able to determine that a number of potentially relevant files had been permanently deleted from the computers and were not recoverable using forensic techniques. The trial court imposed monetary sanctions, but refused plaintiff's request for terminating sanctions since plaintiff had not established that the executive's actions would prevent plaintiff from establishing any of its claims or defenses. The Court of Appeal affirmed [*Oz Optics v. Zeynep* (Cal App 2009), 2009 Cal App Unpub LEXIS 2952] .

13.05[2] Negligent Destruction May Be Sanctionable. Negligent destruction of ESI also may result in sanctions. *CCP § 2023.030(a)* does not require a misuse of the discovery process to be willful before monetary sanctions may be imposed [*Kohan v. Cohan* (1991) 229 CA3d 967, 971, 280 CR 474 CR474 (interpreting former *CCP § 2023(b)(1)*)].

Distinguish:

There is no tort remedy for first-party or third-party negligent spoliation of evidence [*Coprish v. Superior Court* (2000) 80 CA4th 1081, 1090, 95 CR2d 884] .



90 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 13 Seeking or Opposing Sanctions for Noncompliance
II. DETERMINING WHETHER GROUNDS FOR SANCTIONS EXIST

1-13 MB Practice Guide: CA E-Discovery and Evidence 13.06

13.06 Sanctions Against Third-Party Spoliators Are Limited.

Most of the sanctions obtainable under *CCP* § 2023.030 cannot be used against a third-party spoliator--they are available only against a party to the underlying lawsuit [see *Temple Cmty. Hosp. v. Superior Court* (1999) 20 C4th 464, 482-483, 84 CR2d 852, 976 P2d 223 (issue, evidence, and terminating sanctions available only against party)]. Only monetary and contempt sanctions may be imposed against third parties who flout the discovery process by suppressing or destroying evidence [*Temple Cmty. Hosp. v. Superior Court* (1999) 20 C4th 464, 477, 84 CR2d 852, 976 P2d 223] .



91 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 13 Seeking or Opposing Sanctions for Noncompliance
II. DETERMINING WHETHER GROUNDS FOR SANCTIONS EXIST

1-13 MB Practice Guide: CA E-Discovery and Evidence 13.07

13.07 Safe Harbor Protects Good Faith Loss of ESI.

Absent exceptional circumstances, a court may not impose sanctions on a party or any attorney of a party for failure to provide ESI that has been lost, damaged, altered, or overwritten as the result of the routine, good faith operation of an electronic information system [*CCP* § 2031.060(i); *see also CCP* §§ 1985.8(l); 2031.300(d), 2031.310(j); 2031.320(d)].

A similar safe harbor exists under federal law [*see Fed R Civ P 37(e)*]. Under that rule, the good faith requirement has been interpreted to mean "that a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve" [*Keithley v. Home Store.com, Inc.* (ND Cal 2008) 2008 US Dist LEXIS 61741 (quoting *Fed R Civ P 37* Advisory Committee Notes (2006 Amendment))].

Courts have found that parties who fail to impose a litigation hold and continue to destroy ESI after receiving notice of litigation are not acting in good faith and cannot take advantage of the safe harbor [*see, e.g., Doe v. Norwalk Community College* (D Conn 2007) 248 FRD 372, 379 (defendants' failure to place a litigation hold and to preserve e-mails and hard drives relevant to litigation was at least grossly negligent, if not reckless)].

Example:

The court ordered defendants to preserve and produce server log data that was temporarily stored only in defendants' servers' random access memory (RAM) but declined to impose evidentiary sanctions for defendants' failure to retain the data previously. In the absence of (1) prior precedent directly on point in the discovery context, (2) a specific request to preserve the data present solely in RAM, and (3) a violation of a preservation order, defendants were protected by *Fed R Civ P 37*'s safe harbor because their failure to retain the data in RAM was based on a good faith belief that preservation of data temporarily stored only in RAM was not required [*Columbia Pictures Indus. v. Bunnell* (CD Cal 2007) 2007 US Dist LEXIS 46364, *54-55] .



92 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 13 Seeking or Opposing Sanctions for Noncompliance
II. DETERMINING WHETHER GROUNDS FOR SANCTIONS EXIST

1-13 MB Practice Guide: CA E-Discovery and Evidence 13.08

13.08 Types of Sanctions for Spoliation.

13.08[1] Monetary Sanction. The court may impose a monetary sanction ordering that one engaging in the misuse of the discovery process, or any attorney advising that conduct, or both, pay the reasonable expenses, including attorney's fees, incurred by anyone as a result of that conduct [CCP § 2023.030(a)]. The amount of the sanction is limited to the opposing party's expenses actually incurred [see *Ghanooni v. Super Shuttle of Los Angeles* (1993) 20 CA4th 256, 262-263, 24 CR2d 501 (trial court erred in imposing additional sanction unrelated to actual expenses defendants incurred as a result of plaintiff's failure to cooperate with discovery)].

Prerequisite:

Unlike monetary sanctions against a party, which are based on the party's misuse of the discovery process, monetary sanctions against the party's attorney require a finding that the attorney advised the misconduct [CCP § 2023.030(a); *Ghanooni v. Super Shuttle of Los Angeles* (1993) 20 CA4th 256, 261, 24 CR2d 501 (citing *Corns v. Miller* (1986) 181 CA3d 195, 200, 226 CR 247 (construing similar language in former CCP § 2034(b)(2)(D)))].

Examples:

- In a patent infringement case, plaintiffs failed to produce more than 46,000 e-mails and documents that were requested in discovery and that they had agreed to produce. Finding that plaintiffs had not presented any evidence attempting to explain or justify its failure to produce the documents, and that the failure to produce the documents case significantly increased the scope, complexity and length of the litigation, the court ordered plaintiffs to pay defendants all of their attorney's fees and costs, which totaled more than \$8.5 million [*Qualcomm Inc. v. Broadcom Corp.* (SD Cal 2008) 2008 US Dist LEXIS 911, *33-63, vacated in part, *Qualcomm Inc. v. Broadcom Corp.* (SD Cal 2008) 2008 U.S. Dist. LEXIS 16897].

- In a copyright infringement case, defendants violated the court's preservation order by reinstalling operating systems on three of their computers. Plaintiffs argued that the reinstallation showed willful disregard of the preservation order, but defendants claimed that the reinstallation was necessary for the testing and installation of new software. In addition, defendants failed to preserve a notebook computer

that contained an employee's notes of his daily activities, which might have included information about the installation of the new software. Plaintiffs sought monetary and issue sanctions and an adverse inference instruction. The court declined to order the issue sanction or adverse inference instruction, but ordered monetary sanctions in the amount of the cost of analyzing the servers that had been copied but not yet analyzed, which would produce more precise information about the installation of the software. The court awarded additional monetary sanctions for the defendants' failure to preserve the notebook computer, in the amount of one-quarter of the costs incurred by plaintiff in bring the motion for sanctions, plus the cost of reviewing hundreds of defendants' e-mails for evidence of the software installation, which could have been reduced significantly or obviated entirely if the notebook included detailed records of such installation [*Creative Sci. Sys. v. Forex Capital Mkts., LLC* (ND Cal 2006) 2006 US Dist LEXIS 20116, *19-24] .

13.08[2] Issue Sanction. A court may impose an issue sanction ordering that designated facts be taken as established, or precluding the offending party from supporting or opposing designated claims or defenses [CCP § 2023.030(b); *Cedars-Sinai Med. Ctr. v. Superior Court* (1998) 18 C4th 1, 12, 74 CR2d 248, 954 P2d 511] .

Examples:

- In a trademark infringement action, the defendant failed to conduct an adequate search for internal e-mails, resulting in the loss of (1) evidence showing whether the defendant deliberately bid on its own competitors' trademarks, which supported plaintiff's unclean hands or estoppel claim, and (2) documents related to the strength of the claimed trademarks (one of the factors in establishing trademark infringement). The court ordered it judicially established that (1) the defendant bid on its competitors' trademarks to entice persons looking for the websites of those competitors to visit the defendant's website, and (2) the strength of trademark factor weighed in favor of the plaintiff [*Google Inc. v. Am. Blind & Wallpaper Factory, Inc.* (ND Cal 2007) 2007 US Dist LEXIS 48309, *17-21] .

- Defendant's chief executive deliberately wiped the hard drive of his computer after receiving a litigation hold notice from his company's counsel. In the litigation, plaintiff was claiming that defendant had failed to return confidential information plaintiff had electronically provided to defendant in connection with soliciting an investment to fund plaintiff's reorganization, and that defendant had misused the information to compete with plaintiff. The court held that defendant should have done more than merely issue a litigation hold notice, and "should have taken reasonable steps to prevent all of its employees from doing wrongful and foolish things, like destroying evidence, under the pressure of litigation." The court imposed issue sanctions by ordering it established as a matter of fact that defendant had misappropriated the confidential information. However, the court refused to issue terminating sanctions, principally because defendant's chief executive had acted alone and there was no indication anybody else at the company had participated in his destruction of evidence [*Hawaiian Airlines, Inc. v. Mesa Air Group, Inc.* (In re Hawaiian Airlines, Inc.) (Bankr DHa 2007) 2007 Bankr LEXIS 3679] .

13.08[3] Evidence Sanction. The court may prohibit the offending party from introducing designated matters into evidence [CCP § 2023.030(c); *Cedars-Sinai Med. Ctr. v. Superior Court* (1998) 18 C4th 1, 12, 74 CR2d 248, 954 P2d 511] .

Example:

In response to a request for production of documents in an insurance coverage action, the insurer represented to the insured and to the court that no daily activity logs or telephone record logs were created or maintained in connection with plaintiff's claim. In the following months, the insurer belatedly produced those records from a computerized database, causing depositions of claims examiners to be rescheduled. Based on the insurer's past failure to timely produce electronically stored information, and

the insured's concern that additional responsive electronically stored information might be in the insurer's possession, the magistrate judge recommended to the district court that the insurer be precluded from relying on or introducing any documents, testimony, or expert witness testimony that relied on documents or electronically stored information that was requested by the insured but was not produced by the insurer by the discovery deadline [*R & R Sails, Inc. v. Ins. Co.* (SD Cal 2008) 251 FRD 520, 528] .

13.08[4] Adverse Inference. Spoliation may result in the evidentiary inference that evidence that a party has destroyed or rendered unavailable was unfavorable to that party [*Evid Code* §§ 412-413; *Cedars-Sinai Med. Ctr. v. Superior Court* (1998) 18 C4th 1, 11, 74 CR2d 248, 954 P2d 511] . The standard California jury instruction on the inference is as follows: "You may consider whether one party *intentionally* concealed or destroyed evidence. If you decide that a party did so, you may decide that the evidence would have been unfavorable to that party" [*Judicial Council of California Civil Jury Instructions, CACI No. 204* (NexisNexis) (emphasis added)]. Similarly, *Evid Code* § 413 allows a jury to consider a party's "*willful* suppression of evidence" when considering what inferences to draw from the evidence or facts in the case against a party. Thus it appears that, under California state law, negligence or gross negligence is not enough for the imposition of an adverse inference instruction. Evidence of intentional destruction or willful suppression of evidence appears to be required.

Distinguish--California Federal District Courts Have Imposed Adverse Inferences for Negligent Conduct:

In contrast, federal district courts in California have followed the Second Circuit's approach in *Residential Funding Corp. v. DeGeorge Financial Corp.* (2d Cir 2002) 306 F.3d 99 , in which the court stated that "[t]he sanction of an adverse inference may be appropriate in some cases involving the negligent destruction of evidence because each party should bear the risk of its own negligence" [*Residential Funding Corp.* (2d Cir 2002) 306 F.3d 99, 108] . For example, one California federal district court has held that "[t]he culpable state of mind [necessary for an adverse inference instruction] includes negligence" [*Lewis v. Ryan* (SD Cal 2009) 261 FRD 513, 521 (noting that California district courts had followed the Second Circuit's approach in the *Residential Funding* case)]. Federal District Judge Shira Schindlein of the Southern District of New York, the author of the influential *Zubulake* I through IV opinions, has applied the Second Circuit's approach and granted an instruction that the jury is permitted to draw an adverse inference about documents that were destroyed through plaintiff's "gross negligence" when the plaintiffs "failed to timely institute written litigation holds and engaged in careless and indifferent collection efforts after the duty to preserve arose" [*Pension Committee of the University of Montreal et al. v. Banc of America Securities, LLC et al.* (SDNY January 2010) 2010 U.S. Dist. LEXIS 4546, *6, *105-*107] .

Examples:

- In a patent infringement action in which defendants failed to preserve a database containing early versions of relevant source code, the court ordered that the jury be instructed that if plaintiffs proved infringement for later periods for which electronically stored information was available, the jury should infer that infringement occurred during the earlier period as well [*Keithley v. Home Store.com, Inc.* (ND Cal 2008) 2008 US Dist LEXIS 61741, at *50-54] .

- An adverse inference instruction was warranted against a defendant who was at a minimum grossly negligent in allowing relevant documents and e-mails of approximately 44 key players to be destroyed [*Gordon Partners, et. al. v. Blumenthal* (In re NTL, Inc. Sec. Litig.) (SDNY 2007) 244 FRD 179, 200-201] .



Strategic Point--Argue Against Inference When Conduct Is Not Willful:

Evid. C § 413 requires willful conduct. Thus, counsel can argue against the imposition of an adverse inference instruction if the evidence does not show willful conduct. Counsel should argue that the willfulness requirement means that California state courts should not follow the practice of the federal district courts in California, but instead should follow the practice of courts in the Fifth Circuit, which have held that "the adverse inference to be drawn from destruction of records is predicated on bad conduct of the defendant. Moreover, the circumstances of the act must manifest bad faith. Mere negligence is not enough, for it does not sustain an inference of consciousness of a weak case" [*Rimkus Consulting Group, Inc. v. Cammarata* (SD Tex. 2010) 688 F Supp2d 598, 613-614 , internal citations omitted (factual questions whether destruction of ESI was willful or merely negligent were left to jury; judge issued adverse inference instruction similar to CACI No. 204 informing jury that if it found that the defendants intentionally deleted evidence to prevent its use in anticipated or pending litigation, the jury may, but was not required to, infer that lost evidence would have been unfavorable to defendants)]].

Jury Instruction:

Willful Suppression of Evidence, see *Judicial Council of California Civil Jury Instructions*, CACI No. 204 (LexisNexis).

13.08[5] Terminating Sanction. The court may impose terminating sanctions that include striking part or all of the pleadings, staying further proceedings until an order for discovery is obeyed, dismissing part or all of the action, or granting a default judgment against the offending party [CCP § 2023.030(d)]. Terminating sanctions are to be used sparingly and only when the trial court concludes that lesser sanctions would not bring about the compliance of the offending party [*R.S. Creative, Inc. v. Creative Cotton, Ltd.* (1999) 75 CA4th 486, 496, 89 CR2d 353] .

Examples:

- The court granted a terminating sanction, striking defendants' cross-complaints and answer and ordering defendants' default entered, after defendants repeatedly failed to comply with discovery orders and intentionally destroyed evidence requested by plaintiffs by running a program to erase e-mails from computer hard drives [*Electronic Funds Solutions, LLC v. Murphy* (2005) 134 CA4th 1161, 1183-1184, 36 CR3d 663] .

- In a breach of contract case, plaintiffs incorporated a forged contract in their complaint. They then stipulated that certain computers would not be used until defendants' computer expert could examine them, but defendants' examination showed that they had been used and the hard drive wiped clean or replaced. Finally, plaintiffs refused to allow the completion of a deposition. The Court of Appeal held that the trial court was fully justified in dismissing plaintiffs' complaint as a sanction [*R.S. Creative, Inc. v. Creative Cotton, Ltd.* (1999) 75 CA4th 486, 496-498, 89 CR2d 353] .

- In a copyright infringement case, defendant deleted e-mails related to the merits of the action that it was obligated to preserve and produce to plaintiffs. The district court concluded that although plaintiffs were prejudiced by the destruction of evidence, defendant's behavior did not constitute a pattern of deliberately deceptive litigation practices that were likely to continue as the action proceeded. The court therefore denied plaintiffs' request for a default sanction and awarded lesser sanctions [*UMG Recordings, Inc. v. Hummer Winblad Venture Partners (In re Napster, Inc. Copyright Litig.)* (ND Cal 2006) 462 F Supp2d 1060, 1077-1078)] .

13.08[6] Contempt Sanction. The court may impose a contempt sanction by an order treating the misuse of the

discovery process as a contempt of court [CCP § 2023.030(e); see *Newland v. Superior Court* (1995) 40 CA4th 608, 610, 47 CR2d 24 (in appropriate case, failure to pay ordered sanction is punishable as contempt)]. Although the statutory language authorizes use of the contempt power to enforce civil discovery, the use of that drastic sanction in this context is rare [see *In re De La Parra* (1986) 184 CA3d 139, 143-145, 228 CR 864 (refusal to answer interrogatories did not warrant contempt sanction and imprisonment)].



Warning:

Although discovery sanctions against attorneys generally are exempt from the requirement of referring them to the State Bar, the exception does not apply to sanctions for contempt, even if they pertain to the misuse of discovery [see *B&P Code* § 6086.7(a)(1), (3)].

13.08[7] An Attorney May Be Disciplined for Spoliation. An attorney may be subject to discipline, including suspension and disbarment, for participating in the suppression or destruction of evidence [*B&P Code* § 6106 (act of moral turpitude, dishonesty, or corruption is cause for disbarment or suspension); *Cal Rules Prof Conduct*, Rules 5-200 (lawyer may not seek to mislead court by false statement of fact or law), 5-220 (lawyer may not suppress evidence that the lawyer or the lawyer's client has legal obligation to reveal or to produce), 3-210 (lawyer may not advise violation of any law)].

Example:

In a patent infringement case, plaintiff failed to produce more than 46,000 e-mails and documents that were requested in discovery and that plaintiff had agreed to produce. The court found that the plaintiff's outside attorneys had assisted their client in committing this incredible discovery violation by intentionally hiding or recklessly ignoring relevant documents, ignoring or rejecting numerous warning signs that the plaintiff's document search was inadequate, and blindly accepting the plaintiff's unsupported assurances that its document search was adequate. The attorneys then used the lack of evidence to repeatedly and forcefully make false statements and arguments to the court and jury. The court therefore referred the attorneys to the State Bar for potential discipline for violations of Rules 5-200 and 5-220 [*Qualcomm Inc. v. Broadcom Corp.* (SD Cal 2008) 2008 US Dist LEXIS 911, *64 , vacated in part, *Qualcomm Inc. v. Broadcom Corp.* (SD Cal 2008) 2008 U.S. Dist. LEXIS 16897] .

13.08[8] Criminal Penalties Are Available for Willful Spoliation. Willfully destroying or concealing evidence with the intent thereby to prevent it from being produced is a misdemeanor [*Pen Code* § 135].



93 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 13 Seeking or Opposing Sanctions for Noncompliance
II. DETERMINING WHETHER GROUNDS FOR SANCTIONS EXIST

1-13 MB Practice Guide: CA E-Discovery and Evidence 13.09

13.09 A Party May Be Sanctioned for Disobeying a Discovery Order or Unsuccessfully Making or Opposing a Motion to Compel.

13.09[1] Unsuccessful Party in Motion to Compel Response to Inspection Demand Is Subject to Mandatory Monetary Sanction. The court is required to impose a monetary sanction under *CCP § 2023.010 et seq.* against any party, person, or attorney who unsuccessfully makes or opposes a motion to compel a response to an inspection demand [*CCP § 2031.300(c)*].

Exception:

The sanction will not be imposed if the court finds that the one subject to the sanction acted with substantial justification or that other circumstances make the imposition of the sanction unjust [*CCP § 2031.300(c)*].



Timing:

While normally it is advisable to file a motion for sanctions concurrently with the motion to compel responses (or the opposition to a motion to compel responses), the motion for sanctions may be filed at a later time [*London v. Dri-Honing Corp. (2004) 117 CA4th 999, 1007-1008, 12 CR3d 240*] .



Cross Reference:

Discussion of procedure for bringing motion for sanctions, see *13.12*.

13.09[2] Party That Disobeys Order Compelling Response Is Subject to Issue, Evidence, or Terminating Sanction and Monetary Sanction. If a party fails to obey an order compelling a response to an inspection demand, the court may make those orders that are just, including the imposition of an issue sanction, an evidence sanction or a terminating sanction under *CCP § 2023.010 et seq.* [*CCP § 2031.300(c)*].

In lieu of or in addition to that sanction, the court may impose a monetary sanction under *CCP § 2023.010 et seq.* [*CCP § 2031.300(c)*].

Exceptions--Prior Order May Not Be Necessary:

- A stipulation signed by both parties setting a deadline for providing overdue responses was held to be tantamount to the court order compelling responses required by *CCP § 2031.300(c)* [*Mileikowsky v. Tenet Healthsystem* (2005) 128 CA4th 262, 278-280, 26 CR3d 831 (trial court did not err in granting terminating sanctions even though stipulation was never signed by court or filed)].
- A prior court order is not necessary for the imposition of issue and evidence sanctions against a party who has engaged in a pattern of willful discovery abuse that caused the unavailability of evidence [*Karlsson v. Ford Motor Co.* (2006) 140 CA4th 1202, 1215, 45 CR3d 265] .
- When a prior order compelling a response would have been futile, courts have imposed evidence sanctions without such an order.

Examples:

- An order requiring plaintiffs to produce a promised audit report would have been futile because plaintiffs conceded the audit had not been and would not be completed [*Do It Urself Moving & Storage, Inc. v. Brown, Leifer, Slatkin & Berns* (1992) 7 CA4th 27, 35-36, 9 CR2d 396 , superseded on summary judgment issue by amendments to *CCP § 437c*].
- After plaintiffs served the defendant with three separate requests for production of documents and received repeated assurances from the defendant that all documents had been produced, plaintiffs were not required to move to compel further responses before the court could impose evidence sanction [*Pate v. Channel Lumber Co.* (1997) 51 CA4th 1447, 1456, 59 CR2d 919] .

13.09[3] Unsuccessful Party in Motion to Compel Further Response to Inspection Demand Is Subject to Mandatory Monetary Sanction. The court is required to impose a monetary sanction under *CCP § 2023.010 et seq.* against any party, person, or attorney who unsuccessfully makes or opposes a motion to compel further response to an inspection demand [*CCP § 2031.310(d)*].

Exception:

The sanction will not be imposed if the court finds that the one subject to the sanction acted with substantial justification or that other circumstances make the imposition of the sanction unjust [*CCP § 2031.310(d)*].

13.09[4] Party That Disobeys Order Compelling Further Response Is Subject to Issue, Evidence, or Terminating Sanction and Monetary Sanction. If a party fails to obey an order compelling further response, the court may make those orders that are just, including the imposition of an issue sanction, an evidence sanction, or a terminating sanction under *CCP § 2023.010 et seq.* [*CCP § 2031.310(e)*].

In lieu of or in addition to that sanction, the court may impose a monetary sanction under *CCP § 2023.010* [*CCP § 2031.310(e)*].

13.09[5] Unsuccessful Party in Motion to Compel Compliance With Inspection Demand Is Subject to Mandatory Monetary Sanction. The court is required to impose a monetary sanction under *CCP § 2023.010 et seq.* against any party, person, or attorney who unsuccessfully makes or opposes a motion to compel compliance with an inspection demand [*CCP § 2031.320(b)*].

Exception:

The sanction will not be imposed if the court finds that the one subject to the sanction acted with substantial justification, or that other circumstances make the imposition of the sanction unjust [*CCP* § 2031.320(b)].

13.09[6] Party That Disobeys Order Compelling Inspection Is Subject to Issue, Evidence, or Terminating Sanction and Monetary Sanction. If a party fails to obey an order compelling inspection, the court may make those orders that are just, including the imposition of an issue sanction, an evidence sanction, or a terminating sanction under *CCP* § 2023.010 *et seq.* [*CCP* § 2031.320(c)].

In lieu of or in addition to that sanction, the court may impose a monetary sanction under *CCP* § 2023.010 *et seq.* [*CCP* § 2031.320(c)].



94 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 13 Seeking or Opposing Sanctions for Noncompliance
II. DETERMINING WHETHER GROUNDS FOR SANCTIONS EXIST

1-13 MB Practice Guide: CA E-Discovery and Evidence 13.10

13.10 Failure to Return Inadvertently Disclosed Privileged Information Can Result in Disqualification of Counsel.

If a lawyer receives a document in the course of discovery that appears to be protected by the attorney-client privilege or is protected attorney work product, and it is apparent that the materials were provided or made available through inadvertence, the lawyer receiving the documents should refrain from examining the materials and promptly notify the sender that he or she possesses material that appears to be privileged [*Rico v. Mitsubishi Motors Corp.* (2007) 42 C4th 807, 817, 68 CR3d 758, 171 P3d 1092 ; *State Comp. Ins. Fund v. WPS, Inc.* (1999) 70 CA4th 644, 656-657, 82 CR2d 799] . Failure to take such steps can result in disqualification of counsel [*Rico v. Mitsubishi Motors Corp.* (2007) 42 C4th 807, 819, 68 CR3d 758, 171 P3d 1092] .

➡ **Cross Reference:**

Discussion of procedure for recovering inadvertently produced privileged electronically stored information under CCP § 2031.285, see Ch. 3, 3.15.



95 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 13 Seeking or Opposing Sanctions for Noncompliance

III. PROCEDURE FOR SEEKING SANCTIONS

1-13 MB Practice Guide: CA E-Discovery and Evidence 13.11

13.11 CHECKLIST: Procedure for Seeking Sanctions.

☐ Prepare moving papers:

- ☐ Notice of motion.
- ☐ Supporting memorandum.
- ☐ Declaration, if seeking monetary sanction.
- ☐ Separate statement, if seeking issue or evidence sanction.
- ☐ Supporting evidence, if seeking default judgment.
- ☐ Proposed order.



Timing:

Motion for sanctions can be filed concurrently with motion to compel (or opposition to motion to compel), or at later time.

Authority:

CCP §§ 585(b), 2023.040; Cal Rules Ct, Rule 3.1345; London v. Dri-Honing Corp. (2004) 117 CA4th 999, 1007-1008, 12 CR3d 240

Discussion:

See 13.12

Forms:

See 13.20-13.22

☐ If seeking contempt sanction, prepare declaration or affidavit and order to show cause.

Authority:

CCP §§ 1211(a), 1212, 2015.5

Discussion:

See 13.13

Forms:

See 13.23



96 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 13 Seeking or Opposing Sanctions for Noncompliance
III. PROCEDURE FOR SEEKING SANCTIONS

1-13 MB Practice Guide: CA E-Discovery and Evidence 13.12

13.12 Motion for Order Imposing Issue, Evidence, or Terminating Sanction and Monetary Sanction.**13.12[1] Moving Papers.**

13.12[1][a] Notice of Motion. A request for a sanction must identify, in the notice of motion, every person, party, and attorney against whom the sanction is sought and specify the type of sanction sought [CCP § 2023.040].

**Strategic Point:**

A motion for sanctions may request a range of sanctions in the alternative, e.g., for issue and evidentiary sanctions, or alternatively a terminating sanction [see, e.g., *Walker v. San Francisco Hous. Auth.* (2002) 100 CA4th 685, 690, 122 CR2d 758 ; *R.S. Creative, Inc. v. Creative Cotton, Ltd.* (1999) 75 CA4th 486, 493, 89 CR2d 353 (defendants moved for terminating sanctions or, alternatively, for lesser sanctions)].

Prerequisite:

Sanctions may not be imposed ex parte; written notice in accordance with CCP § 1005 is required [*Parker v. Wolters Kluwer United States, Inc.* (2007) 149 CA4th 285, 296, 57 CR3d 18] .

**Timing:**

While normally it is advisable to file a motion for sanctions concurrently with the motion to compel responses (or the opposition to a motion to compel responses), the motion for sanctions may be filed at a later time [*London v. Dri-Honing Corp.* (2004) 117 CA4th 999, 1007-1008, 12 CR3d 240] .

**Cross Reference:**

Form, see 13.20.

13.12[1][b] Notice of Motion Must Be Supported by Memorandum. The notice of motion must be supported by a memorandum [CCP § 2023.040; see also CCP §§ 1005(b), 1010; *Cal Rules Ct, Rule 3.1113(a)* (memorandum in support of motion)].

**Cross Reference:**

Forms for supporting motions for discovery sanctions, see *California Points and Authorities*, § 82.10 (Matthew Bender).

13.12[1][c] Notice of Motion Must Be Accompanied by Declaration If Monetary Sanction Is Sought. The notice of motion must be accompanied by a declaration setting forth facts supporting the amount of any monetary sanction sought [*CCP* § 2023.040].

13.12[1][d] Notice of Motion for Issue or Evidence Sanction Must Be Accompanied by Separate Statement. A motion for issue or evidence sanctions must be accompanied by a separate statement [*Cal Rules Ct, Rule 3.1345(a)(7)*]. No separate statement is required when no response has been provided to the request for discovery [*Cal Rules Ct, Rule 3.1345(b)*].

A separate statement is a separate document filed and served with the discovery motion that sets forth all the information necessary to understand each discovery request and all the responses to it that are at issue. The separate statement must be full and complete so that no person is required to review any other document to determine the full request and the full response. Material may not be incorporated by reference [*Cal Rules Ct, Rule 3.1345(c)*].

The separate statement must include, for each discovery request, the following [*Cal Rules Ct, Rule 3.1345(c)*]:

- The text of the request, interrogatory, question, or inspection demand.
- The text of each response, answer, or objection, and any further responses or answers.
- A statement of the factual and legal reasons for compelling further responses, answers, or production as to each matter in dispute.
- If necessary, the text of all definitions, instructions, and other matters required to understand each discovery request and the responses to it.
- If the response to a particular discovery request depends on the response given to another discovery request, or if the reasons a further response to a particular discovery request is deemed necessary are based on the response to some other discovery request, the other request and the response to it must be set forth.
- If the pleadings, other documents in the file, or other items of discovery are relevant to the motion, the party relying on them must summarize each relevant document.

Cross Reference:

Form, see 13.21.

13.12[1][e] Default Judgment Requires Supporting Evidence. A party may obtain a default judgment under *CCP* § 585(b) after the entry of default only on application to the court and after a hearing. When requesting a terminating sanction of default, the moving party should review this provision, which governs default judgments generally [see *Lang v. Hochman* (2000) 77 CA4th 1225, 1240-1241, 92 CR2d 322 (default judgment prove-up hearing scheduled after hearing resulting in terminating sanctions)].

Cross Reference:

Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure, Ch. 36, Defaults and Motions for Relief.

13.12[2] Order.

13.12[2][a] Losing Party Should Request Written Findings. When written findings are not required, the losing party should request them [see *Estate of Ruchti* (1993) 12 CA4th 1593, 1604, 16 CR2d 151] .

13.12[2][b] Written Findings Are Required When Mandatory Monetary Sanctions Are Not Imposed. As a general rule, findings are not required for the imposition of monetary sanctions [see *California Shellfish Inc. v. United Shellfish Co.* (1997) 56 CA4th 16, 26 (citing *Ghanooni v. Super Shuttle of Los Angeles* (1993) 20 CA4th 256, 261, 24 CR2d 501)]. However, when monetary sanctions are mandatory absent "substantial justification," written findings are impliedly required if the sanction is *not* imposed [see *California Shellfish, Inc. v. United Shellfish Co.* (1997) 56 CA4th 16, 26, 64 CR2d 797 (because court found appellant acted with "substantial justification" and did *not* impose monetary sanctions, express findings were not required); *Estate of Ruchti* (1993) 12 CA4th 1593, 1603, 16 CR2d 151 (due process does not require written findings when imposing monetary sanctions, even if mandatory))].

13.12[2][c] Imposition of Monetary Sanctions Against Attorney Requires Finding. Unlike monetary sanctions against a party, which are based on the party's misuse of the discovery process, monetary sanctions against the party's attorney require a finding that the attorney advised the conduct [see CCP § 2023.030(a); *Ghanooni v. Super Shuttle of Los Angeles* (1993) 20 CA4th 256, 261, 24 CR2d 501 .

**Strategic Point:**

An attorney attempting to establish that he or she did not advise the conduct in question may need to rely on information protected by the attorney-client privilege. If the client does not agree to waive the privilege, the attorney can attempt to rely on the "self-defense" exception to the attorney-client privilege [see *Qualcomm Inc. v. Broadcom Corp.* (SD Cal 2008) 2008 U.S. Dist. LEXIS 16897] .

**Cross References:**

Discussion of asserting self-defense exception to attorney-client privilege, see 13.15[1][c].

Form, see 13.22.



97 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 13 Seeking or Opposing Sanctions for Noncompliance
III. PROCEDURE FOR SEEKING SANCTIONS

1-13 MB Practice Guide: CA E-Discovery and Evidence 13.13

13.13 Order to Show Cause for Contempt.

13.13[1] Affidavit Required for Indirect Contempt. When a contempt of court is not committed in the immediate view and presence of the court, or of the judge at chambers, an affidavit must be presented to the court or judge of the facts constituting the contempt (alternatively, a statement of the facts by the referees or arbitrators, or other judicial officers may be presented) [CCP § 1211(a); see CCP § 2015.5 (certification under penalty of perjury)].

Procedurally, punishment for an indirect contempt begins with the presentation of an affidavit setting forth the alleged contemptuous acts. The affidavit is, in effect, a complaint that frames the issues before the court. It is a jurisdictional prerequisite to the court's power to punish [CCP § 1211(a); *Moss v. Superior Court* (1998) 17 C4th 396, 401-402, n1, 71 CR2d 215, 950 P2d 59] .

13.13[2] Notice or Order to Show Cause Required. When a contempt of court is not committed in the immediate view and presence of the court or of the judge, a warrant of commitment may be granted on notice or on an order to show cause [CCP § 1212 (also providing for warrant of attachment); see also *Cedars-Sinai Imaging Med. Group v. Superior Court* (2000) 83 CA4th 1281, 1286 n5, 100 CR2d 320] .

➡ **Cross Reference:**

Form, see 13.23.

13.13[3] Personal Service and Full Hearing Required. A court may not punish a contempt committed out of its presence without a full hearing at which the contemner appears after having been personally served with the affidavit and order to show cause [*Lund v. Superior Court* (1964) 61 C2d 698, 713, 39 CR 891, 394 P2d 707 ; *Cedars-Sinai Imaging Med. Group v. Superior Court* (2000) 83 CA4th 1281, 1286, 100 CR2d 320] .

Exception--Service on Attorney When Contemner Concealed:

When the alleged contemner is concealing himself or herself to avoid service of an order to show cause, or remains outside the state for that purpose, the court may direct that service be made on the contemner's attorney of record [*Kroneberger v. Superior Court* (1961) 196 CA2d 206, 210, 16 CR 339 ; see CCP § 1015 (service on attorney); see also *Cedars-Sinai Imaging Med. Group v. Superior Court* (2000) 83 CA4th 1281, 1287, 100 CR2d 320] .

13.13[4] Judgment of Contempt.

13.13[4][a] Judgment Must Specify Act and Include Finding That Act Is Within Contemner's Power. A judgment of contempt must not only specify the act to be performed, but must also include a finding that the act is within the power of the contemner to perform [*Nutter v. Superior Court* (1960) 183 CA2d 72, 75, 6 CR 404] .

The defendant must have the ability to comply with the order [*Mitchell v. Superior Court* (1989) 49 C3d 1230, 1256, 265 CR 144, 783 P2d 731 (pornographic theater manager did not have control over performing employees); *In re Cassil* (1995) 37 CA4th 1081, 1087, 44 CR2d 267] .

13.13[4][b] Judgment Should Contain Factual Findings. While an indirect contempt judgment need not recite the court's factual findings as a jurisdictional prerequisite, those findings should be specifically recited orally or in the judgment to assist a reviewing court [see *Moss v. Superior Court* (1998) 17 C4th 396, 404 n3, 71 CR2d 215, 950 P2d 59] .

 Cross References:

Form, see 13.23.

DeMeo, *California Deposition and Discovery Practice*, § 42.10 (Matthew Bender).



98 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 13 Seeking or Opposing Sanctions for Noncompliance
IV. OPPOSING IMPOSITION OF SANCTIONS

1-13 MB Practice Guide: CA E-Discovery and Evidence 13.14

13.14 CHECKLIST: Opposing Imposition of Sanctions.

☐ If motion for sanctions was filed, determine whether grounds exist to object to moving papers or motion procedure.

- ☐ Determine whether notice was sufficient.
- ☐ Determine whether procedure provides for opportunity to be heard.
- ☐ Determine whether motion is in proper form.

Authority:

CCP §§ 2023.030, 2023.040

Discussion:

See 13.15

☐ If monetary sanctions are sought, determine grounds for opposition:

- ☐ Determine whether substantial justification exists for conduct.
- ☐ Determine whether circumstances exist that would make imposition of sanction unjust.
- ☐ Review moving party's declaration and determine whether:
 - ☐ Expenses sought are reasonable and related to the discovery abuse described or, rather, punitive, which is inappropriate.

☐ Reasonable expenses are itemized and explained.

☐ Pro se litigant is seeking reasonable expenses that do not include attorney's fees.

☐ In the case of sanctions against the attorney, establish, if applicable, that attorney did not advise conduct.

Authority:

CCP § 2023.030(a)

Discussion:

See 13.15[1]

☐ If issue, evidence, or terminating sanction is sought, determine grounds for opposition:

☐ Consider any mistaken impression or honest confusion that resulted in conduct.

☐ Consider explanation for conduct that would render conduct understandable or less egregious

☐ Consider whether, under circumstances, the less drastic imposition of monetary sanctions would be more appropriate.

☐ Be prepared to argue that the more serious sanctions sought are too extreme and that lesser sanctions would achieve objective of protecting interests of opposing party.

Authority:

CCP § 2023.030; Hartbrodt v. Burke (1996) 42 CA4th 168, 173, 49 CR2d 562

Discussion:

See 13.15[2]

☐ If order to show cause for contempt was filed with respect to an indirect contempt, determine whether proper procedures were followed:

☐ Determine whether alleged contemner was personally served or whether his or her attorney was served if he or she was avoiding service.

☐ Determine whether alleged contemner is being afforded a full hearing.

☐ Determine whether order to show cause was based on sufficient affidavit.

☐ Consider arguing that less serious sanctions are more appropriate.

Authority:

CCP §§ 1015, 1211(a), 2015.5, 2023.030; Kroneberger v. Superior Court (1961) 196 CA2d 206, 210, 16 CR 339

Discussion:

See 13.15[4]



99 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 13 Seeking or Opposing Sanctions for Noncompliance
IV. OPPOSING IMPOSITION OF SANCTIONS

1-13 MB Practice Guide: CA E-Discovery and Evidence 13.15

13.15 Options and Strategies for Opposing Imposition of Sanctions.

13.15[1] Opposing Imposition of Monetary Sanction.

13.15[1][a] Showing Substantial Justification to Render Mandatory Imposition of Monetary Sanction

Unjust. The court will impose mandatory monetary sanctions when authorized unless the losing party convinces the court that the party acted with "substantial justification or that other circumstances make the imposition of the sanction unjust" [see *CCP § 2023.030(a)*; *California Shellfish, Inc. v. United Shellfish Co. (1997) 56 CA4th 16, 25-26, 64 CR2d 797*]. Inasmuch as monetary sanctions under *CCP § 2023.030(a)* (and as authorized in particular discovery proceedings) are considered the least severe form of discovery sanction, the party requesting such sanctions has relatively light burdens of proof and persuasion. Thus, the opposing party's burden is met by showing substantial justification or other circumstances rendering the sanction unjust.

13.15[1][b] Limiting Amount of Sanction to Reasonable Expenses. A monetary sanction for misuse of the discovery process is limited to the opposing party's reasonable expenses, including attorney's fees, incurred as a result of that conduct [see *CCP § 2023.030(a)*]. In a motion for monetary sanctions, the requesting party must submit a declaration setting forth facts supporting the amount sought [see *CCP § 2023.040*]. Opposing counsel should challenge any unreasonable or unsupported expenses by filing a counter-declaration [*London v. Dri-Honing Corp. (2004) 117 CA4th 999, 1010*].

Example:

A monetary award against the plaintiff consisting of \$2,100 for attorney fees and costs defendants incurred in the preparation and argument of the motion to compel was proper. However, the trial court's *additional* \$1,000 monetary award against plaintiff to punish her failure to cooperate with defendants' discovery was error because it was unrelated to the actual expenses defendants incurred [*Ghanooni v. Super Shuttle of Los Angeles (1993) 20 CA4th 256, 262-263, 24 CR2d 501*].

➡ Cross References:

Discussion of monetary sanctions, see *13.08[1]*.

Discussion of declaration of expenses, see *13.12[1]*.

Form for memorandum opposing motion for monetary sanction, see *California Points and Authorities*, Ch. 82, *Discovery: Sanctions for Discovery Misuse*, § 82.30 (Matthew Bender).

13.15[1][c] Opposing Sanction Against Attorney on Ground That Attorney Did Not Advise Conduct. Unlike monetary sanctions against a party, which are based on the party's misuse of the discovery process, monetary sanctions against the party's attorney require a finding that the attorney advised that conduct [CCP § 2023.030(a); *Ghanooni v. Super Shuttle of Los Angeles* (1993) 20 CA4th 256, 261, 24 CR2d 501 (citing *Corns v. Miller* (1986) 181 CA3d 195, 200, 226 CR 247, which construed similar language in former CCP § 2034(b)(2)(D))]. Counsel who did not advise the client's conduct may be able to support that assertion by reference to the court record of the discovery proceedings in question.



Strategic Point:

An attorney attempting to establish that he or she did not advise the conduct in question may need to rely on information protected by the attorney-client privilege. If the client does not agree to waive the privilege, the attorney can attempt to rely on the "self-defense" exception to the attorney-client privilege [see *Evid Code* § 958 (no privilege as to communication relevant to an issue of breach by the lawyer of a duty arising out of the lawyer-client relationship)]. For example, in *Qualcomm Inc. v. Broadcom Corp.*, the court found that the plaintiff's attorneys had assisted their client in withholding more than 46,000 e-mails and documents from discovery and referred the attorneys to the State Bar for potential discipline for violations of Rules 5-200 and 5-220. The attorneys brought a motion for a finding of a federal common law self-defense exception to their client's asserted attorney-client privilege, which the court granted once there was a showing of adversity between the attorneys and their client [*Qualcomm Inc. v. Broadcom Corp.* (SD Cal 2008) 2008 U.S. Dist. LEXIS 16897] . (The attorneys subsequently managed to convince the district court that although there were "ineffective and problematic interactions between Qualcomm employees and most of the attorneys during the pretrial litigation," the attorneys had "made significant efforts to comply with their discovery obligations." After considering the new facts, the district court declined to sanction any of the outside counsel attorneys [*Qualcomm Inc. v. Broadcom Corp.* (SD Cal April 2, 2010) 2010 U.S. Dist. LEXIS 33889, *9] .)



Cross Reference:

Form for memorandum opposing motion for monetary sanction, see *California Points and Authorities*, Ch. 82, *Discovery: Sanctions for Discovery Misuse*, § 82.21 (Matthew Bender).

13.15[1][d] Opposing Imposition of Attorney's Fees Incurred by Pro Se Litigant. If the party seeking the monetary sanction of reasonable attorney's fees is acting in propria persona, he or she is not entitled to *attorney's fees*, but may recover other reasonable expenses actually incurred, such as photocopying, computer-assisted legal research, and other identifiable and allocable costs [see *Kravitz v. Superior Court* (2001) 91 CA4th 1015, 1020-1021, 111 CR2d 385 ; *Argaman v. Ratan* (1999) 73 CA4th 1173, 1180, 86 CR2d 917] . As with all reasonable expenses constituting monetary sanctions, a written declaration is prerequisite to recovery [see CCP § 2023.040].

13.15[2] Opposing Imposition of Issue, Evidence, or Terminating Sanction.

13.15[2][a] Issue, Evidence, and Terminating Sanctions Are Serious Sanctions, Not to Be Considered Lightly. Issue, evidence, and terminating sanctions under the Discovery Act are considered the "serious" available sanctions [see, e.g., *Maldonado v. Superior Court* (2002) 94 CA4th 1390, 1399, 115 CR2d 137 ; *Newland v. Superior Court* (1995) 40 CA4th 608, 613, 47 CR2d 24 (sanctions are listed in graduated severity, beginning with monetary awards and ending with terminating orders)]. Imposition of issue or evidence sanctions may be tantamount to a terminating sanction, since they may completely undermine a party's case and lead directly to an adverse judgment. Therefore, an attorney opposing a motion for sanctions should carefully document and present all mitigating circumstances or

mistaken impressions that apply [see, e.g., *Hartbrodt v. Burke* (1996) 42 CA4th 168, 173, 49 CR2d 562 (plaintiff's refusal to produce vital tape recording led to terminating sanction and dismissal)].

A motion for any of these sanctions is not a trivial matter, especially if the record reflects multiple instances of discovery abuse [see, e.g., *Collisson & Kaplan v. Hartunian* (1994) 21 CA4th 1611, 1616, 26 CR2d 786 (terminating sanctions proper when obtaining discovery was "like pulling teeth")].

13.15[2][b] Less Drastic Alternatives May Be Appropriate. As an alternative to opposing the imposition of any sanctions, a party may assert that issue, evidence, or terminating sanctions are too extreme under the circumstances. Counsel should argue that less drastic alternatives exist that would remedy the particular abuse [see, e.g., *Hartbrodt v. Burke* (1996) 42 CA4th 168, 173, 49 CR2d 562 (although plaintiff asserted that less drastic alternatives to dismissal would be appropriate, court disagreed)]. The most commonly imposed lesser sanction is a monetary sanction against the party or the attorney who advised the conduct [see CCP § 2023.030(a)].



Warning:

A plaintiff cannot defeat defendant's motion for a terminating discovery sanction by filing a voluntary dismissal without prejudice [*Hartbrodt v. Burke* (1996) 42 CA4th 168, 168-175, 176, 49 CR2d 562] .



Cross Reference:

Forms for memoranda opposing motions for discovery sanctions, see *California Points and Authorities*, Ch. 82, *Discovery: Sanctions for Discovery Misuse*, §§ 82.20-82.22, 82.31.

13.15[3] Opposing Imposition of Sanction for Misuse of Discovery Process on Ground of Improper Notice or Absence of Opportunity for Hearing.

13.15[3][a] Party Opposing Sanction May Object to Notice and Absence of Opportunity to Be Heard.

Discovery sanctions for misuse of the discovery process under CCP § 2023.010 *et seq.* may be imposed only after notice to any affected party, person, or attorney, and after opportunity for a hearing [see CCP § 2023.030]. A sanction order issued *ex parte* is void [*Parker v. Wolters Kluwer United States, Inc.* (2007) 149 CA4th 285, 296, 57 CR3d 18] . A person subject to the imposition of discovery sanctions may raise any defect in those requirements as a ground for opposition to those sanctions.

13.15[3][b] Party Opposing Sanction May Object to Noncompliance With Statutory Motion Requirements.

A motion for imposition of discovery sanctions must comply with the requirements set forth in CCP § 2023.040. A person subject to the imposition of discovery sanctions may raise any failure to comply with those requirements as a ground for opposition to those sanctions.



Cross Reference:

See 13.12.

13.15[4] Opposing Contempt Sanction.

13.15[4][a] Person Cannot Be Punished for Indirect Contempt in Absence of Personal Service and Full Hearing for Indirect Contempt. A person subject to an order to show cause for contempt who has not been personally served or afforded a full hearing may oppose the proceeding on those grounds [see CCP §§ 1211(a) (affidavit required), 2015.5 (certification under penalty of perjury); *Lund v. Superior Court* (1964) 61 C2d 698, 713, 39 CR 891, 394 P2d 707; *Cedars-Sinai Imaging Med. Group v. Superior Court* (2000) 83 CA4th 1281, 1287, 100 CR2d 320] .

The requirements of notice and hearing are jurisdictional. Inasmuch as the contempt proceeding is punitive and separate from the cause out of which it arose, the prescribed procedural safeguards must be accorded the alleged contemner [

Kroneberger v. Superior Court (1961) 196 CA2d 206, 210, 16 CR 339]. In a contempt proceeding, every "i" must be dotted and every "t" crossed [see *Cedars-Sinai Imaging Med. Group v. Superior Court* (2000) 83 CA4th 1281, 1287, 100 CR2d 320].

Exception--Service on Attorney When Contemner Concealed:

An alleged contemner, however, may be served through his or her attorney if he or she has been concealing himself or herself to avoid service, or remains outside the state for that purpose [*Kroneberger v. Superior Court* (1961) 196 CA2d 206, 210, 16 CR 339 ; see CCP § 1015 (service on attorney); see also *Cedars-Sinai Imaging Med. Group v. Superior Court* (2000) 83 CA4th 1281, 1286-1287, 100 CR2d 320].

13.15[4][b] Person Cannot Be Punished for Indirect Contempt in Absence of Sufficient Affidavit. If an order to show cause for contempt is not supported by a sufficient affidavit, or if the order is not signed by a judge, the alleged contemner may oppose the proceeding on those grounds [CCP § 1211(a); see CCP § 2015.5 (certification under penalty of perjury)]. Any question as to the adequacy of the order to show cause and the affidavit and declaration on which it was based should be raised by an appropriate pleading in response to that order [*Morelli v. Superior Court* (1968) 262 CA2d 262, 266, 68 CR 572].

13.15[4][c] Contempt Sanction for Discovery Enforcement Is Drastic. Although the statutory language authorizes use of the contempt power to enforce civil discovery, the use of that drastic sanction in this context is rare [see *In re De La Parra* (1986) 184 CA3d 139, 143-144, 228 CR 864]. A party subject to a contempt sanction in this context may always argue that procedure is too drastic, especially if the public interests are not at issue [see, e.g., *In re De La Parra* (1986) 184 CA3d 139, 143-144, 228 CR 864 (discussing rare use of incarceration under contempt sanction in criminal trial involving news reporter's rights under *US Const. amend I*)].

13.15[4][d] Person Is Not Subject to Contempt for Failing to Perform Act That He or She Is Incapable of Performing. A judgment of contempt must not only specify the act to be performed, it must also include a finding that the act is within the power of the contemner to perform [*Nutter v. Superior Court* (1960) 183 CA2d 72, 75, 6 CR 404].

A person must have the ability to comply with the order [*Mitchell v. Superior Court* (1989) 49 C3d 1230, 1255-1256, 265 CR 144, 783 P2d 731 ; *In re Cassil* (1995) 37 CA4th 1081, 1087, 44 CR2d 267].

Example:

It is not a contempt of court for a party to fail to pay a sum, however small, when it is not in his or her power so to do [*Nutter v. Superior Court* (1960) 183 CA2d 72, 75, 6 CR 404].

13.15[4][e] Affidavit in Opposition Should Set Forth Facts Explaining Circumstances. A person opposing a contempt sanction should file an affidavit in opposition, setting forth the circumstances of the conduct, e.g., explaining an inability to comply with an order, if appropriate [see, e.g., *Nutter v. Superior Court* (1960) 183 CA2d 72, 74, 6 CR 404 (in family law proceeding, husband subject to contempt explained that he did not have financial ability to pay child support award)].



Cross References:

California Forms of Pleading and Practice, Ch. 135, Contempt (Matthew Bender).

Forms for memoranda opposing motions for discovery sanctions, see *California Points and Authorities*, Ch. 82, *Discovery: Sanctions for Discovery Misuse*, §§ 82.20-82.22, 82.31 (Matthew Bender).



100 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 13 Seeking or Opposing Sanctions for Noncompliance

IV. OPPOSING IMPOSITION OF SANCTIONS

1-13 MB Practice Guide: CA E-Discovery and Evidence 13.16 -13.19

[Reserved]

13.16[Reserved]



101 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 13 Seeking or Opposing Sanctions for Noncompliance
V. FORMS

1-13 MB Practice Guide: CA E-Discovery and Evidence 13.20

13.20 Notice of Motion, Motion, and Supporting Declaration for Imposition of Issue, Evidence, or Terminating Sanction, and Monetary Sanctions Based on Discovery Misuse.

Notice of Motion, Motion, and Supporting Declaration for Imposition of Issue, Evidence, or Terminating Sanction, and Monetary Sanctions Based on Discovery Misuse.

SUPERIOR COURT OF CALIFORNIA,
COUNTY OF FARALLON

_____ [name], Plaintiff vs. _____ [name], Defendant.	)) No. ____) NOTICE OF MOTION AND MOTION FOR OR-) DER IMPOSING _____ [specify types) of sanctions requested, e.g. , MONETARY AND IS-) SUE] SANCTIONS AGAINST _____ [identify party,) e.g., DEFENDANT] _____ [name],) [AND IMPOSING MONETARY SANCTIONS) AGAINST _____ (identify) attorney)] FOR FAILURE TO OBEY ORDER COM-) PELLING _____ [specify, e.g., IN- SPECTION OF DOCUMENTS], SUPPORTING DE- CLARATION OF _____ [name], STATEMENT OF _____ [name], AND MEMORANDUM IN SUPPORT OF MOTION Date: _____ Time: _____ Location: _____ Judge: _____ Date Action Filed: _____ Trial Date: _____

To _____ [identify party, e.g., Defendant Mary Jones] and to his/her attorney of record:

NOTICE IS HEREBY GIVEN that on _____ [date], at _____ [time], or as soon thereafter as the matter may be heard, in [_____ (Department or Division) _____ of] this court, located at _____ [street address], _____ [identify party, e.g., Plaintiff John Smith] will, and hereby does, move for an order that _____ [specify, e.g., issue, evidence, and terminating] sanctions be imposed against _____ [identify party, e.g., Defendant Mary Jones], specifically that _____ [specify order sought, e.g., Defendant Mary Jones be prohibited from introducing the following matters in evidence in this action: _____]. _____ [Identify moving party, e.g., Plaintiff John Smith] will further move for an order imposing a monetary sanction against _____ [identify persons, e.g., Defendant Mary Jones and her attorney Jane Lee] and in favor of _____ [identify moving party, e.g., Plaintiff John Smith] in the amount of \$_____. The motion will be made on the ground that _____ [identify party, e.g., Defendant Mary Jones] has failed to obey the order of this court dated _____ [date] compelling _____ [specify, e.g., preservation of evidence stored on computers in her custody or control] by _____ [specify, e.g., reinstalling operating systems on three computers containing electronically stored information subject to the aforementioned order of this court, resulting in a loss of data].

The motion will be based on this notice of motion, on the declaration of _____ [name] served and filed herewith pursuant to *CCP § 2023.040*, on the separate statement of _____ [name] served and filed herewith pursuant to *Cal Rules Ct, Rule 3.1345(a)(7)*, on the memorandum served and filed herewith, on the records and files herein, and on such evidence as may be presented at the hearing of the motion.

Dated: _____

_____ [firm name, if any]

By: _____ [signature]

_____ [typed name]

Attorney for _____

[moving party's status or name]

SUPPORTING DECLARATION OF _____ [name]

I _____ [name], declare:

1. I am _____ [identify declarant, e.g., an attorney at law duly admitted to practice before all the courts of the State of California and the attorney of record herein for Plaintiff, Mary Jones].

2. On _____ [date], this court entered an order compelling _____ [identify party, e.g., Defendant Mary Jones] to _____ [describe order, e.g., produce documents in response to Demand No. 3 in Plaintiff John Smith's First Set of Demands for Inspection on or before December 20, 2009], a copy of which is attached as Exhibit A and incorporated by reference.

3. _____ [Identify party, e.g., Defendant Mary Jones] has failed to _____ [describe order, e.g., produce responsive documents] in a proper manner in that _____ [describe insufficiency of lack of compliance, e.g., she failed to produce any emails sent or received by her during 2007].

4. As a result of the failure of _____ [identify party, e.g., Defendant Mary Jones] to obey the above-described court order, _____ [identify moving party, e.g., Plaintiff John Smith] has incurred

expenses as follows: _____ [*itemize and explain reasonable expenses, including attorney's fees*], for a total of \$_____

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

_____ [date]
_____ [signature]
_____ [typed name]

MEMORANDUM IN SUPPORT OF MOTION

[Add memorandum supporting motion.]

NOTES:

Authority:

CCP § 2023.040

Grounds:

See 13.04, 13.05, 13.09

Related Form for Separate Statement:

See 13.21

Related Form for Order:

See 13.22

Related Form for Memorandum:

See *California Points and Authorities, Ch. 82, Discovery: Sanctions for Discovery Misuse, § 82.11*
(Matthew Bender)



102 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 13 Seeking or Opposing Sanctions for Noncompliance
V. FORMS

1-13 MB Practice Guide: CA E-Discovery and Evidence 13.21

13.21 Separate Statement Supporting Motion for Issue or Evidence Sanction.

Separate Statement Supporting Motion for Issue or Evidence Sanction.
SUPERIOR COURT OF CALIFORNIA,
COUNTY OF FARALLON

	)	
	)	No. _____
	)	SEPARATE STATEMENT IN SUPPORT OF MO-
	)	TION FOR ORDER IMPOSING ISSUE OR EVID-
_____ [name], Plaintiff vs.	)	ENCE SANCTION
_____ [name], Defendant.	)	Date: _____
	)	Time: _____
	)	Location: _____
	)	Judge: _____
	)	Date Action Filed: _____
	)	Trial Date: _____

This separate statement is submitted in support of the motion by _____ [identify moving party, e.g., Plaintiff John Smith] for an order imposing on _____ [identify party, e.g., Defendant Mary Jones] issue and monetary sanctions. As required under *Cal Rules Ct, Rule 3.1345*, it provides information relating to the discovery requests at issue in the motion, as follows: _____ [specify particular discovery request, e.g., Plaintiff's Demand No. 3 in Plaintiff John Smith's First Set of Demands for Inspection]

1. The text of the discovery request: _____ [set forth text, e.g., all documents containing daily logs or telephone records relating to Plaintiff's claim for coverage].

[2. The special instructions required to understand this demand for inspection are: _____ (set forth instructions).]

[3. Definitions required to understand this demand for inspection request are: _____ (set forth definitions,

e.g., "document" is a writing as defined in *California Evidence Code Section 250* and includes the original or a copy of handwriting, typewriting, printing, photostating, photographing, and every other means of recording any tangible thing and form of communicating or representation, including letters, words, pictures, sounds, or symbols or combinations of them).]

4. The text of the response(s): _____ [set forth text of response, and any further responses, to the specific request, *e.g.*, Defendant has no documents responsive to this Request.].

[5. Related pleadings and other documents are as follows: _____ (summarize any pleadings or other documents in the file, if any, that are relevant to the motion and are relied on by the moving party).]

Dated: _____

_____ [firm name, if any]

By: _____ [signature]

_____ [typed name]

Attorney for _____

[moving party's status or name]

NOTES:

Authority:

Cal Rules Ct, Rule 3.1345

Related Form for Notice of Motion:

See 13.20



103 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 13 Seeking or Opposing Sanctions for Noncompliance
V. FORMS

1-13 MB Practice Guide: CA E-Discovery and Evidence 13.22

13.22 Order on Motion for Imposition of Issue, Evidence or Terminating Sanction, and Monetary Sanction.

Order on Motion for Imposition of Issue, Evidence or Terminating Sanction, and Monetary Sanction.
SUPERIOR COURT OF CALIFORNIA,
COUNTY OF FARALLON

_____ [name], Plaintiff vs.	)	
_____ [name], Defendant.	)	No. _____
	)	ORDER
	)	

The motion of _____ [identify moving party, e.g., Plaintiff John Smith] for an order imposing an issue, evidence, and terminating sanction against _____ [identify party, e.g., Defendant Mary Jones] and imposing a monetary sanction against _____ [identify persons, e.g., Defendant Mary Jones and her attorney Jane Lee], for failure to obey the order of this court dated _____ [date], compelling _____ [specify, e.g., preservation of evidence stored on computers in her custody or control], came on regularly for hearing on _____ [date]. Plaintiff appeared by counsel _____ [name, e.g., Tom Doe]; Defendant appeared by counsel _____ [name, e.g., Jane Lee].

On proof being made to the satisfaction of the court _____ [state findings of court, e.g., Defendant Mary Jones failed to obey the order of this court dated November 15, 2009, compelling her to preserve all evidence stored on computers in her custody or control by _____ [specify, e.g., reinstalling operating systems on three computers containing electronically stored information subject to the aforementioned order of this court, resulting in a loss of data], and that her counsel Jane Lee advised her to disobey this order, and on this court's finding that the requested order ought to be granted],

[EITHER]

IT IS ORDERED that the motion be, and hereby is, denied.

[OR]

IT IS ORDERED that the motion be, and hereby is, granted and that _____ [*specify order, e.g.,* Defendant is prohibited from introducing the following matters in evidence in this action: _____].

[EITHER]

IT IS FURTHER ORDERED that _____ [*specify persons subject to monetary sanction, e.g.,* Defendant Mary Jones and her attorney Jane Lee] pay forthwith to John Smith] the sum of \$_____ as reasonable expenses and attorney's fees.

[OR]

On further proof made to the satisfaction of the court that _____ [*specify, e.g.,* Defendant Mary Jones and her attorney Jane Lee] [*acted with substantial justification or set forth other circumstances making imposition of sanctions unjust*],

[CONTINUE]

IT IS FURTHER ORDERED that no monetary sanction be imposed on _____ [*specify, e.g.,* Defendant Mary Jones and her attorney Jane Lee].

Dated: _____

_____ [*signature*]
Judge of the Superior Court

NOTES:

Authority:

CCP § 2023.040

Related Form for Notice of Motion:

See 13.20



104 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 13 Seeking or Opposing Sanctions for Noncompliance
V. FORMS

1-13 MB Practice Guide: CA E-Discovery and Evidence 13.23

13.23 Order to Show Cause Re Contempt and Supporting Declaration.

Order to Show Cause Re Contempt and Supporting Declaration.
SUPERIOR COURT OF CALIFORNIA,
COUNTY OF FARALLON

	)	
	)	No. _____
	)	DECLARATION OF _____ [name]
	)	AND ORDER TO SHOW CAUSE RE CONTEMPT
_____ [name], Plaintiff vs.	)	Date: _____
_____ [name], Defendant.	)	Time: _____
	)	Location: _____
	)	Judge: _____
	)	Date Action Filed: _____
	)	Trial Date: _____

DECLARATION OF _____ [name]

I _____ [name], declare:

1. I am _____ [identify declarant, e.g., an attorney at law duly admitted to practice before all the courts of the State of California and the attorney of record herein for Plaintiff, John Smith].

2. On _____ [date], _____ [set forth facts describing initiation of discovery, e.g., plaintiff served a notice of taking the deposition of Paul Green at 100 North Main Street, Suite 200, Farallon City, California, on December 3, 2009, at 10:00 A.M. True copies of this notice and proof of service are attached hereto as Exhibits A and B, respectively, and made a part of this order].

[EITHER, if contempt order is sought for disobedience of deposition subpoena under Code Civ. Proc. § 2020.240 or 2025.440(b)]

3. _____ [Set forth facts showing issuance of a deposition subpoena and cited person's consequent failure to attend or to be sworn as a witness].

[OR, if contempt order is sought for disobedience by deponent of order compelling answer or production of items under Code Civ. Proc. § 2025.480(g)]

3. _____ [Set forth facts describing order compelling an answer to a deposition question, or production of a writing or tangible thing under the deponent's control, and cited person's failure to comply therewith, e.g. , On _____ [date], this court ordered Paul Green to produce within seven days printouts of all computerized databases containing daily logs or telephone records maintained by Green and pertaining to Plaintiff's claim for coverage. Green has failed to produce any printout.].

[CONTINUE]

4. _____ [At all times mentioned in this order or at the time he/she was to perform the acts described above, Paul Green has/had the ability to do so.]

5. _____ [Name of person to be cited]'s failure to act as described above has been willful and with the intent to frustrate the processes of this court and to deprive _____ [identify party seeking contempt order, e.g., Plaintiff] of the benefits to which he/she is entitled under the order, in that _____ [describe].

6. _____ [Set out expenses].

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Dated: _____

_____ [signature]

_____ [typed name]

ORDER TO SHOW CAUSE

To _____ [name of person to be cited] and to _____ [name], his/her attorney of record.

IT IS HEREBY ORDERED that you, _____ [name of person to be cited], appear in _____ (Department or Division) _____ of] this court, located at _____ [address], on _____ [date], at _____ [time], then and there to show cause, if any, why an order should not be made adjudging you to be in contempt and punished for that contempt, pursuant to Section _____ [2020.240 or 2025.440(b) or 2025.480(g)] of the Code of Civil Procedure, for your failure to _____ [specify, e.g. , attend the taking of your deposition on December 20, 2009, at 10.00 A.M., at 100 North Main Street, Suite 200, Farallon City, California, (location), pursuant to the deposition subpoena issued out of and by the clerk of this court], of which you were duly notified, as set out in the declaration of _____ [name], served with this order.

[IT IS FURTHER ORDERED that at the time and place stated above you show cause why you should not be required

to pay to _____ (*identify party seeking contempt order, e.g. , Plaintiff John Smith the reasonable expenses including attorney's fees that he/she incurs in obtaining an order of this court adjudging you in contempt, which expenses are set out in the attached declaration of John Smith.*)

IT IS FURTHER ORDERED that the service of this order to show cause and a copy of the supporting declaration of _____ [*name*] be made on _____ [*name of person to be cited*] at least _____ [*name of person to be cited*] days before the date and time set for the hearing of this order to show cause.

Dated: _____

_____ [*signature*]

Judge of the Superior Court

NOTES:

Authority:

CCP §§ 1209(a)(5), 2020.240, 2023.040, 2025.440(b), 2025.480(g)

Related Form for Memorandum:

See California Points and Authorities, Ch. 82, Discovery: Sanctions for Discovery Misuse, § 82.15
(Matthew Bender)



105 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.syn

AUTHOR: Diane E. Barry, Esq.

§ 14.syn Synopsis to Chapter 14: Discovery of Electronically Stored Information Residing in Foreign Jurisdictions

14.01 Scope.

14.02 Objective and Strategy.

14.03 CHECKLIST: Analyzing Applicable California Law Regarding Discovery of ESI Residing Abroad.

14.04 Objective and Strategy.

14.05 Discovery of Foreign Persons May Be Available Under California Code of Civil Procedure.

14.05[1] Counsel Should First Try to Obtain ESI Under California Code of Civil Procedure.

14.05[2] Recent Case Law Supports Availability of Discovery Against Foreign Residents Under California Law.

14.06 Foreign Nationals Can Request Use of Hague Convention for Evidence.

14.06[1] Foreign Party Can Object to Discovery Under California Law.

14.06[2] Burden of Persuasion Is on Party Desiring to Invoke Hague Convention.

14.06[3] Court Must Undertake Comity Analysis to Determine Applicable Rules.

14.06[4] Comity Analysis Must Consider Specified Factors.

14.06[5] Existence of Blocking Statutes in Foreign Nation Does Not Necessarily Bar Use of California Code of Civil Procedure.

14.06[6] If California Court Orders Production Under Code of Civil Procedure, Foreign Party Must Comply or Face

Sanctions.

14.07 Jurisdiction Must Be Obtained.

14.07[1] Jurisdiction Over Foreign Person in California Court Requires Appropriate Service of Process and Sufficient Minimum Contacts.

14.07[2] Party Seeking Discovery Must Obtain Service of Process on a Foreign Person or Corporation.

14.07[2][a] Usual Methods Apply for Service Within California.

14.07[2][b] Service Outside California but Inside United States Can Be Made Under Law of California or Other State.

14.07[2][c] Choices Exist for Service Outside of the United States.

14.07[2][d] Procedure for Service of Process Under Hague Convention.

14.07[3] Jurisdiction in California Court Requires Minimum Contacts Analysis.

14.08 CHECKLIST: Conducting Foreign E-Discovery Using the Hague Convention.

14.09 Objective and Strategy.

14.10 Treaties and Other Agreements Set Scope of International Discovery.

14.10[1] Treaties Define Scope of International Discovery.

14.10[2] Hague Convention for Evidence Can Be Used to Obtain ESI.

14.11 Hague Convention on Taking of Evidence Abroad in Civil or Commercial Matters--General Principles and Structure.

14.11[1] Hague Convention Was Intended to Assist Transfer of Evidence Materials Between Civil Law and Common Law Nations.

14.11[2] Letters of Request Under Hague Convention for Evidence Are Preferable to Letters Rogatory If Discovery Under California Code of Civil Procedure Is Not Available.

14.11[3] Application Limited to Hague Convention Signers.

14.11[4] Availability of Pre-Trial Discovery Is Limited in Many Hague Convention Nations.

14.11[4][a] Hague Convention for Evidence Permits Contracting States to File Reservations Limiting Pre-Trial Discovery.

14.11[4][b] Letter of Request Must Relate to Pending or Contemplated Judicial Proceeding.

14.11[5] Costs of Letter of Request Procedure Should Be Evaluated.

14.12 Letter of Request Must Be Sent to Foreign Nation.

14.12[1] Party Seeking Discovery Must Have California Court Issue Letter of Request.

14.12[2] Party Seeking Discovery Must Prepare and File Motion to Issue Letter of Request in California Court.

14.12[3] Party Seeking Discovery Must Prepare Form for Letter of Request.

14.12[3][a] Party Should Prepare Letter of Request Form for Court's Signature.

14.12[3][b] ESI Should Be Described As Specifically As Possible to Maximize Possibility of Success.

14.12[3][c] Letter of Request May Ask That Particular Procedures Be Followed.

14.12[3][d] Letter of Request Must Meet Hague Convention Language Requirements.

14.12[4] California Court Forwards Letter of Request to Designated Central Authority of Foreign Nation.

14.13 Foreign Nation Will Act on Letter of Request.

14.13[1] Central Authority May Raise Objections to Letter and Must Notify California Authority of Objections.

14.13[2] Central Authority Will Forward Letters of Request to Appropriate Local Authority in Foreign Nation for Execution.

14.13[3] Receiving Nation Will Use Its Own Procedures, but Will Consider Procedural Requests.

14.13[4] Receiving Nation Must Enforce Letter of Request As It Would Similar Domestic Requests.

14.13[5] Requesting Authority Must Be Informed If Letter of Request Cannot Be Executed.

14.13[6] Local Authority Will Enforce or Refuse to Comply With Letter of Request.

14.13[6][a] Local Authority Serves Letter of Request on ESI Custodian.

14.13[6][b] Custodian of ESI Can Object Under Local Law.

14.14 CHECKLIST: Conducting Foreign E-Discovery Using Letters Rogatory.

14.15 Objective and Strategy.

14.16 Counsel Should Research Judicial Resources Available to Assist With Letters Rogatory in Recipient Country.

14.16[1] Counsel Should Research Local Law and Judicial Attitudes.

14.16[2] Counsel Should Consider Obtaining Assistance of Foreign Counsel.

14.17 Letters Rogatory May Be Issued Pursuant to a Treaty or in Absence of Treaty.

14.17[1] Letters Rogatory Issued Under Treaty Generally Are Preferable.

14.17[2] Ordinary Letters Rogatory Can Be Issued If No Treaty or Convention Applies.

14.17[3] Party May Request ESI Under Inter-American Convention on Letters Rogatory If Foreign Nation Is a Signatory.

14.18 Preparation and Issuance of Letters Rogatory.

14.18[1] Letters Rogatory Must Be Issued by California Court.

14.18[2] Counsel Should Consult Official Forms in Drafting Letters Rogatory.

14.18[3] Counsel Should Use Appropriate Language.

14.18[3][a] Letter Should Be Drafted in Language of the Receiving Nation.

14.18[3][b] Letter Should Use Non-Technical Language and No Idioms.

14.18[3][c] Letter Should Request Production, Not "Discovery."

14.18[4] Requests for ESI or Documentary Evidence Should Be As Specific As Possible.

14.18[5] Counsel Should Request Specific Procedures If Needed.

14.18[6] Counsel Should Prepare a Motion and Order for California Court to Issue Letters Rogatory.

14.18[7] Appropriate Documents Should Accompany Letters.

14.19 Court Will Forward Letters Rogatory to Foreign Nation.

14.19[1] Letters Rogatory Are Forwarded by Court.

14.19[2] Letters Rogatory Issued Through IACLR May Be Presented Through U.S. State Department or Directly to Executing Nation.

14.19[3] Law and Procedures of Executing Nation Will Be Applied.

14.19[4] Letters Rogatory Will Not Be Executed If Contrary to Public Policy.

14.19[5] Production of ESI Under Letters Rogatory.

14.20 CHECKLIST: Dealing With Foreign Barriers to Pre-Trial Discovery.

14.21 Objective and Strategy.

14.22 Different Types of Foreign Laws Can Block Flow of E-Discovery Materials to United States.

14.22[1] Foreign Laws Governing Citizens' Rights and Privileges Can Conflict With California Discovery Statutes.

14.22[2] Foreign "Blocking Statutes" Can Expressly Target Discovery of Citizens.

14.22[3] Judicial Respect Accorded to Foreign Laws Varies According to Nature and Purpose of Statute.

14.23 The EU Data Privacy Directive and Member Enforcement Laws.

14.23[1] Right to Privacy Is Recognized by European Union.

14.23[2] EU Data Privacy Directive Binds All EU Member States.

14.23[3] Directive Applies to Any Entity Subject to EU Community Law.

14.23[4] Directive Presents Significant Obstacle for Litigation in U.S. Courts.

14.23[5] Directive Regulates Activities of "Controllers" of Regulated Personal Data.

14.23[6] Directive Regulates Processing or Movement of "Personal Data."

14.23[7] Directive Regulates Personal Data Collections and Forbids Later Processing for Different Purposes.

14.23[8] Litigation Production Preparation Steps Are "Processing" Within Meaning of Directive.

14.23[9] Exemptions May Apply to Permit Litigation Processing in Some Situations.

14.23[9][a] Data Subjects Can Consent to Later Processing.

14.23[9][b] Later Processing Permitted to Comply With Legal Obligations.

14.23[9][c] Processing May Be Permitted If Necessary for Controller's Legitimate Interests.

14.23[9][d] Processing May Be Permitted If Necessary for Defense of Legal Claims Within EU.

14.23[10] Directive Also Regulates Cross-Border Movement of Personal Data.

14.23[10][a] Directive Imposes Limitations on Movement of Information.

14.23[10][b] Data May Be Transferred If "Adequate Level of Protection" Exists.

14.23[10][c] United States Is Not an Approved Destination for Personal Data, but Individuals Can Apply for Approval Under Safe Harbor in Directive.

14.23[11] Data Subjects Have Personal Right to Sue for Infringement.

14.24 Blocking Statutes May Pose Barrier to ESI Production.

14.24[1] Blocking Statutes Specifically Address Foreign Litigation.

14.24[2] Blocking Statutes Are Not Always Enforced by Foreign Nation.

14.24[3] United States Courts Accord Lesser Judicial Respect to Blocking Statutes.

14.25 CHECKLIST: Evaluating Practical and Technical Considerations in Foreign E-Discovery

14.26 Objective and Strategy.

- 14.27 Practical Considerations Must Be Considered in Any Cost-Benefit Analysis.
- 14.28 Counsel Must Decide How to Address Technical Collection Issues in Foreign E-Discovery.
- 14.28[1] Counsel Must Decide Whether to Hire Foreign or U.S. Vendors for ESI Collection.
- 14.28[2] Collection Must Be Unicode Compliant.
- 14.29 Counsel Must Decide How to Address Issue of Foreign Language Document Review.
- 14.29[1] Review Must Be Conducted in English, Foreign Language, or a Combination of the Two.
- 14.29[2] Bilingual Staffing May Make Review Much Easier.
- 14.29[3] Translation Is Required If Documents Are Reviewed in English.
- 14.29[4] Search Tools Must Be Selected Carefully.
- 14.29[5] Cross-Lingual Search Tools Are Available.
- 14.29[6] Conceptual Search Tools Allow Concept-Based Searching.
- 14.30 Notice of Motion and Motion for Issuance of Letters Rogatory or Letter of Request.
- 14.31 Proposed Order for Commission, Letters Rogatory, or Letter of Request for Deposition in Foreign Nation.
- 14.32 Letter of Request for Service Abroad, With Certification of Service--Hague Convention Form (U.S. Marshals Service Form USM94).
- 14.33 Model for Letters of Request Recommended for Use in Applying the Hague Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters.
- 14.34 Letters Rogatory--Form A Under Additional Protocol to the Inter-American Commission on Letters Rogatory.
- 14.35 Essential Information for the Addressee--Form B Under Additional Protocol to the Inter-American Commission on Letters Rogatory.
- 14.36 Certificate of Execution--Form C Pursuant to Additional Protocol to the Inter-American Convention on Letters Rogatory

Diane E. Barry, Esq. n*

FOOTNOTES:

(n1)Footnote *. Diane E. Barry, Esq. is the Director of Discovery Strategy and Management at International Litigation Services, Inc. Diane's practice focuses on ESI discovery under state and federal rules of civil procedure, and complex litigation discovery planning and management. Diane assists clients in planning and preparing for ESI discovery conferences and court appearances, as well as preparation for specialized discovery such as IT custodian depositions, key player and IT interviews. In addition, Diane has significant expertise in utilizing technology to improve results in privilege and relevance review. Diane earned her A.B. degree from Vassar College and her J.D. degree, cum laude, from the Boston University School of Law. She holds a professional certification in Data Warehousing from U.C.

Berkeley.



106 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions

I. STRATEGY

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.01

AUTHOR: Diane E. Barry, Esq.

14.01 Scope.

This chapter discusses the basic process for obtaining discovery of ESI residing in foreign jurisdictions, and practical considerations when dealing with foreign-language ESI.

- Practical and technical considerations in foreign discovery [see 14.03--14.07].
- Foreign discovery using the Code of Civil Procedure [see 14.05, 14.06].
- Foreign discovery using the Hague Convention [see 14.08-14.13].
- Foreign discovery using letters rogatory [see 14.14-14.19].
- Foreign barriers to U.S.-style discovery [see 14.20-14.24].
- Practical and Technical Considerations in conducting foreign e-discovery [see 14X.25-14.29].

Core Statutes:

CCP § 413.10 (service of process outside of California); *CCP §§ 2016-2036* (Civil Discovery Act); The Hague Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters; The Hague Convention on Taking of Evidence Abroad in Civil or Commercial Matters; Inter-American Convention on Letters Rogatory; EU Directive 95/46/EC (protection regarding the processing or movement of personal data).



107 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions

I. STRATEGY

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.02

AUTHOR: Diane E. Barry, Esq.

14.02 Objective and Strategy.

Information stored on computers located in jurisdictions outside United States is common in today's business environment. These issues are not confined to federal court; they can and do arise in California civil litigation. Obtaining discovery of electronically stored information located outside the United States presents special problems for the California litigator, and can be a difficult process. Attorneys involved in e-discovery should be familiar with the basic issues and processes involved in conducting such discovery when ESI is stored outside the United States, and to counsel their clients on the difficulties and expense involved.

In addition to the legal framework for acquiring ESI located outside the United States, litigants must consider the practical requirements of dealing with foreign language ESI. Counsel should review Part VI of this chapter [14.25-14.29], regarding the practical considerations of dealing with foreign language ESI, before commencing what may be a lengthy and expensive legal process to obtain it.



108 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
II. ANALYZING APPLICABLE CALIFORNIA LAW REGARDING DISCOVERY OF ESI RESIDING ABROAD

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.03

AUTHOR: Diane E. Barry, Esq.

14.03 CHECKLIST: Analyzing Applicable California Law Regarding Discovery of ESI Residing Abroad.

☐ Is ESI physically located outside United States?

☐ If ESI is owned or controlled by a foreign person (individual or corporate), does foreign person (individual or corporate) have a residence or place of business in California?

Authority:

Volkswagenwerk Aktiengesellschaft v. Schlunk (1988) 486 US 694, 706-708, 108 S Ct 2104, 100 L Ed2d 722

Discussion:

See 14.07[2].

☐ If the ESI is owned or controlled by a foreign person (individual or corporate), does foreign person have sufficient minimum contacts with State of California to support California jurisdiction?

Authority:

Arnesen v. Raymond Lee Org., Inc. (1973) 31 CA3d 991, 996, 107 CR 744

Discussion:

See 14.07[1], 14.07[3]

☐ Is nation where ESI is physically located a civil law nation or a common law nation?

Authority:

Am. Home Assur. Co. v. Societe Commerciale Toutelectric (2002) 104 CA4th 406, 128 CR2d 430

Discussion:

See 14.11[1]

Forms:

See 14.30-14.36

- ☐ Is ESI physically located in a nation that is signatory to Hague Convention for Service, or Hague Convention for Taking of Evidence?

Authority:

Hague Convention for the Service Abroad of Judicial and Extrajudicial Documents [1969 UST LEXIS 152]; Hague Convention for the Taking of Evidence in Civil or Commercial Matters [23 UST 2555; 1970 UST LEXIS 497]

Discussion:

See 14.11[3]

Forms:

See 14.32-14.33

- ☐ Can other parties obtain sufficient pre-trial discovery under Hague Convention for Evidence rather than California Code of Civil Procedure, or will compliance with Hague Convention put them at a disadvantage?

Authority:

Societe Nationale Industrielle Aerospatiale v. United States Dist. Court (1987) 482 US 522, 542, 107 S Ct 2542, 96 L Ed2d 461

Discussion:

See 14.11[4]

Forms:

See 14.32-14.33

- ☐ Is foreign party willing to pay additional expenses that would be imposed through compliance with Hague Convention for Evidence rather than California Code of Civil Procedure?

Authority:

See *Cottle v. Superior Court* (1992) 3 CA4th 1367, 5 CR2d 882 (court's general power to control litigation); see also *Societe Nationale Industrielle Aerospatiale v. US Dist Ct* (1987) 482 US 522, 542, 107 S Ct 2542, 96 L Ed2d 461

Discussion:

See 14.11[5]

- ☐ Will foreign government impose fines or other legal penalties on foreign resident if foreign resident complies with discovery required by California Code of Civil Procedure?

Authority:

Report of United States Delegation to Eleventh Session of Hague Conference on Private

International Law (discussion of problems of sovereign infringement caused by common law discovery practices in civil law nations); see *Am. Home Assur. Co. v. Societe Commerciale Toutelectric (2002)* 104 CA4th 406, 426, 128 CR2d 430

Discussion:

See 14.05[1]

Forms:

See 14.30-14.36



109 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
 II. ANALYZING APPLICABLE CALIFORNIA LAW REGARDING DISCOVERY OF ESI RESIDING ABROAD

*1-14 MB Practice Guide: CA E-Discovery and Evidence 14.04***AUTHOR:** Diane E. Barry, Esq.**14.04 Objective and Strategy.**

Attorneys faced with a situation involving ESI located in a foreign jurisdiction should first review the relevant California statutes and case law governing discovery of evidence, including ESI evidence, residing in foreign jurisdictions. This will give them a basic understanding of the framework of international discovery, and help them decide if it is appropriate to pursue the process.

The initial question is whether it is possible to use California discovery procedures to obtain the ESI. These procedures, if available, are preferable. They provide the broadest scope of discovery as well as the most efficient enforcement procedures. In addition, they are familiar to both counsel and the court. The strongest case for using California's discovery statutes is for those matters in which the desired ESI is located abroad, but is controlled by a party who has been validly served. This approach becomes less certain when the ESI resides abroad but is owned or controlled by non-parties. In either case, the party in possession of the ESI will have potential arguments against the use of the California discovery statutes [see 14.06[1]].

**Strategic Points:**

- The tension in this area of California law pertains to whether a party must, in the first instance, use the Hague Convention for the Taking of Evidence in Civil or Commercial Matters to request production of evidence from a foreign litigant, or whether the party can conduct ordinary discovery under the Code of Civil Procedure. The most recent case law from the California Courts of Appeal states that pursuant to U.S. Supreme Court precedent, the Code of Civil Procedure should be the first resort [*Am. Home Assur. Co. v. Societe Commerciale Toutelectric* (2002) 104 CA4th 406, 128 CR2d 430 ; see *Societe Nationale Industrielle Aerospatiale v. US Dist Ct* (1987) 482 US 522, 107 S Ct 2542, 96 L Ed2d 461] . Older appellate district precedent says the Hague Convention should be used first. There is no ruling available on this point from the California Supreme Court [*Volkswagenwerk v. Sup. Ct* (1981) 123 CA3d 840, 176 CR 874 ; *Pierburg GmbH & Co. KG v. Sup. Ct.* (1982) 137 CA3d 238, 186 CR 876 ; *Volkswagenwerk v. Sup. Ct.* (1973) 33 CA3d 503, 109 CR 219 ; see 14.07 for discussion].

■ The most desirable position is to be able to use the Code of Civil Procedure. The other available methods all cost more in both time and money, have a more limited scope, and have less direct enforcement methods. Demanding parties should take the position that discovery pursuant to the Code of Civil Procedure is the method of first resort according to U.S. Supreme Court and California precedent, and that as necessary, a California court can tailor the Code of Civil Procedure procedures to accommodate foreign comity and sovereignty concerns.



110 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
 II. ANALYZING APPLICABLE CALIFORNIA LAW REGARDING DISCOVERY OF ESI RESIDING ABROAD

*1-14 MB Practice Guide: CA E-Discovery and Evidence 14.05***AUTHOR:** Diane E. Barry, Esq.**14.05 Discovery of Foreign Persons May Be Available Under California Code of Civil Procedure.**

14.05[1] Counsel Should First Try to Obtain ESI Under California Code of Civil Procedure. If the foreign resident is a party to the matter, and the court has properly exercised jurisdiction over the foreign party, inspection requests for production of ESI should be issued pursuant to the ordinary provisions of the Code of Civil Procedure [CCP § 2031.010; *Am. Home Assur. Co. v. Societe Commerciale Toutelectric (2002) 104 CA4th 406, 128 CR2d 430* (Code of Civil Procedure should be first resort for discovery)]. Although there are potential pitfalls in this area, this approach should be tried first with foreign parties to the litigation.

**Strategic Points--Foreign Defendants Can Be More Resistant to Discovery Under Code of Civil****Procedure Than Under International Law:**

- Even if they have no objection to producing the evidence in question, foreign citizens often prefer to supply ESI located in another country under a Hague Convention on Taking of Evidence letter of request, if the foreign country is a signatory to that Convention, or via letters rogatory. This is true even if e-discovery is available under California law and the parties in question can be properly served. Their concern is that foreign governments are less likely to object to a Hague Convention letter of request (or letters rogatory) than to a discovery request under United States law, and therefore less likelihood exists that the responding party will run afoul of the foreign country's privacy and disclosure laws in attempting to comply with the e-discovery request. The worst-case situation dreaded by responding parties is the possibility of conflicting official orders: a foreign government ministry orders non-production, under penalty of monetary sanctions or jail, while a California court orders production of the ESI, under threat of monetary or litigation-ending sanctions in the case of noncompliance. Foreign parties often believe that there is less likelihood of this situation arising if they proceed under the Hague Convention. Thus, it is not unusual for a foreign responding party to resist discovery under California law, but offer to comply if discovery is taken under the Hague Convention (or via letters rogatory, if the nation in question is not a signatory to the Hague Convention for Evidence).

■ These matters can be, and typically are, the subject of informal negotiations among the parties. The requesting party may have considerable negotiating leverage by agreeing to proceed under the Hague Convention rather than the Code of Civil Procedure, in return for full cooperation by the responding party.

► **Cross References:**

Hague convention procedures, see 14.08-14.13.

Letters rogatory, see 14.14-14.19.

Foreign privacy and disclosure laws, see 14.22-14.23.

Discussion of blocking statutes and recognition issues in United States courts, see 14.24.

14.05[2] Recent Case Law Supports Availability of Discovery Against Foreign Residents Under California Law. The weight of current authority appears to support the position that discovery against foreign persons is available under the California Code of Civil Procedure [see discussion below].

The Hague Convention for the Taking of Evidence Abroad in Civil and Commercial Matters ("Hague Convention for Evidence") was formally ratified by the United States Senate, signed by the President, and is part of the laws of the United States. It became effective in the United States as of October 7, 1972 [23 UST 2555]. Between 1973 and 1983, California's First, Second and Third Appellate Districts decided that comity concerns and respect for the sovereignty of foreign nations required that California parties use the Hague Convention for Evidence rather than the Code of Civil Procedure when seeking evidence located abroad [*Volkswagenwerk v. Sup. Ct* (1981) 123 CA3d 840, 176 CR 874 ; *Pierburg GmbH & Co. KG v. Sup. Ct.* (1982) 137 CA3d 238, 186 CR 876 ; *Volkswagenwerk v. Sup. Ct.* (1973) 33 CA3d 503, 109 CR 219] .

In 1987, the United States Supreme Court decided *Societe Nationale Industrielle Aerospatiale v. US Dist Ct* (1987) 482 US 522, 107 S Ct 2542, 96 L Ed2d 461 . In *Aerospatiale*, the Supreme Court held that by its very terms, the Hague Convention for Evidence was an optional method rather than a compulsory one. Therefore, courts should employ their own rules of civil procedure, and address comity concerns as they actually arose. American courts were instructed to be respectful of any "special problems" that confronted a foreign litigant "on account of its nationality or the location of its operations, and for any sovereign interest expressed by a foreign state" [*Societe Nationale Industrielle Aerospatiale v. US Dist Ct* (1987) 482 US 522, 546, 107 S Ct 2542, 96 L Ed2d 461] .

Thereafter, California's First District Appellate Division held that *Aerospatiale* overruled the earlier California precedent, and that the Code of Civil Procedure should be used in the first instance, rather than the Hague Convention for Evidence. California judges can take the difficulties facing foreign litigants into account, but need not use the Hague Convention for Evidence as the mandatory vehicle for discovery in the first instance. Rehearing was denied, and the California Supreme Court refused review [*Am. Home Assur. Co. v. Societe Commerciale Toutelectric* (2002) 104 CA4th 406, 128 CR2d 430 (Hague Convention discovery procedures are not the exclusive means of obtaining evidence from a foreign litigant, and it is not necessary to use these procedures as a matter of first resort)].

► **Cross References:**

The full text of the Hague Convention for Evidence is available on lexis.com at 23 UST 2555; 1970 UST LEXIS 497.

Discovery procedures under Hague Convention for Evidence, see 14.08-14.13.

Examples--Hague Convention for Evidence Rules Are Permissive.

■ In *Societe Nationale Industrielle Aerospatiale v. US Dist Ct* (1987) 482 US 522, 107 S Ct 2542 96 L Ed2d 461, two French corporations designed, manufactured and marketed their aircraft in the United States. After a crash, citizens of Iowa sued the French corporations. When served with requests for production under the Federal Rules of Civil Procedure, the French corporations filed a motion for a protective order on the grounds that the Hague Convention for Evidence was the exclusive vehicle for discovery against them. They also provided proof that a French blocking statute prohibited them from responding to discovery requests other than those propounded under the Hague Convention. The U.S. Supreme Court held that compliance with the Hague Convention for Evidence was not required for taking evidence abroad. The treaty was permissive rather than mandatory. When discovery abroad is required, the District Court ought to scrutinize the particular facts, sovereign interests, and likelihood that resort to the Convention procedures will prove effective. Parties could proceed under the Federal Rules of Civil Procedure, and the federal district court could adjust discovery options if the comity analysis required.

■ In *Am. Home Assur. Co. v. Societe Commerciale Toutelectric* (2002) 104 CA4th 406, 128 CR2d 430, a French corporation wholly owned a Florida corporation that reneged on a construction contract. Initial discovery was conducted under the Code of Civil Procedure. After a fair amount of poor discovery conduct, the French corporation took the position that all further discovery should be conducted through the Hague Convention for Evidence, as that treaty provided the exclusive means for obtaining evidence abroad. In addition, the French Ministry of Justice barred the French corporation from providing the requested discovery, but stated that it might change its decision if the requests were issued pursuant to the Hague Convention for Evidence. When the requested discovery was not produced, the plaintiff successfully moved for terminating sanctions. The appellate court held that *Aerospatiale* governed, and that therefore, a California court was not required to resort to the Hague Convention for Evidence in the first instance. It further held that defendant had waived its right to request resort to the Hague Convention for Evidence by participating in Code of Civil Procedure discovery earlier in the matter. The terminating sanction was upheld.



111 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
II. ANALYZING APPLICABLE CALIFORNIA LAW REGARDING DISCOVERY OF ESI RESIDING ABROAD

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.06

AUTHOR: Diane E. Barry, Esq.

14.06 Foreign Nationals Can Request Use of Hague Convention for Evidence.

14.06[1] Foreign Party Can Object to Discovery Under California Law. A foreign party presented with a demand for discovery (including e-discovery) under California law can request that discovery be conducted under the Hague Convention for Evidence. Such a request may be presented either formally or informally. It can arise informally during the meet and confer process and has been known to take the form of the responding party indicating a willingness to proceed under the Hague Convention process but not under California law. If the parties are unable to resolve the issue informally, a formal objection may be raised with the court [see *Societe Nationale Industrielle Aerospatiale v. US Dist Ct* (1987) 482 US 522, 107 S Ct 2542, 96 L Ed2d 461 ; *Am. Home Assur. Co. v. Societe Commerciale Toutelectric* (2002) 104 CA4th 406, 128 CR2d 430] .

14.06[2] Burden of Persuasion Is on Party Desiring to Invoke Hague Convention. The party wishing to invoke the Hague Convention for Evidence bears the burden of persuasion to show that comity interests favor its application [*Am. Home Assur. Co. v. Societe Commerciale Toutelectric* (2002) 104 CA4th 406, 427, 128 CR2d 430] .

14.06[3] Court Must Undertake Comity Analysis to Determine Applicable Rules. "Comity refers to the spirit of cooperation in which a domestic tribunal approaches the resolution of cases touching the laws and interests of other sovereign states" [*Societe Nationale Industrielle Aerospatiale v. US Dist Ct* (1987) 482 US 522, 544 n 27, 107 S Ct 2542, 96 L Ed2d 461] . Under both *Aerospatiale* and *American Home Assurance*, California courts are required to undertake a comity analysis, and consider the sovereign and important interests of the foreign state and the difficulties these interests impose on a foreign party. Adjustments to the local rules of procedure can be made at the discretion of the court [*Am. Home Assur. Co. v. Societe Commerciale Toutelectric* (2002) 104 CA4th 406, 426, 128 CR2d 430] .

14.06[4] Comity Analysis Must Consider Specified Factors. The court's comity analysis should consider at least the following factors [*Societe Nationale Industrielle Aerospatiale v. US Dist Ct* (1987) 482 US 522, 544 n 28, 107 S Ct 2542, 96 L Ed2d 461 ; see *Richmark Corp. v. Timber Falling Consultants* (9th Cir. 1992) 959 F2d 1468 (making an *Aerospatiale* comity analysis in matter of sanctions against a mainland Chinese corporation.); *Minpeco, S.A. v. ContiCommodity Services, Inc.* (SDNY 1987) 116 FRD 517, 527-528 (comity analysis found that cost in international comity of requiring Swiss bank to violate Swiss law and reveal customer information was greater than benefit to litigation of receiving the discovery)]:

- The importance to the litigation of the ESI, documents or other information requested.
- The specificity of the request.
- Whether the requested information originated in the United States.
- Whether the information is available through alternative means.
- The extent to which noncompliance with the request would undermine important interests of the United States or the State of California.
- The extent to which compliance with the request would undermine important interests of the nation where the information is located.

14.06[5] Existence of Blocking Statutes in Foreign Nation Does Not Necessarily Bar Use of California Code of Civil Procedure. Civil law nations view the taking of evidence and testimony as a solely judicial function [see 14.11[1]]. Judges and other official court officers take evidence. Private citizens do not. Common law nations view civil litigation as a primarily private matter. The individual parties and their counsel should arrange for the exchange of materials and testimony, and the court should be involved as little as possible. Civil law nations view this practice of permitting private citizens to issue broad-based discovery requests as an infringement on the power and authority of the courts and the state. Many civil law nations have passed blocking statutes, the purpose of which is to prevent their citizens from complying with foreign common law-style discovery requests [see 14.24].

The Hague Convention for Evidence was intended to help bridge the gap between these two legal systems, and create methods that both could tolerate [*Societe Nationale Industrielle Aerospatiale v. US Dist Ct* (1987) 482 US 522, 529, 107 S Ct 2542, 2548 ; Report of United States Delegation to Eleventh Session of Hague Conference on Private International Law (discussion of problems of sovereign infringement caused by common law discovery practices in civil law nations)].

However, in *Aerospatiale* and *American Home Assurance*, neither the U.S. Supreme Court nor the California appellate court considered a foreign blocking statute as sufficient cause to require use of the Hague Convention for Evidence over the domestic rules of civil procedure, if the court appropriately considered how to make any required comity adjustments [*Societe Nationale Industrielle Aerospatiale v. US Dist Ct* (1987) 482 US 522, 545, 107 S Ct 2542, 96 L Ed2d 461 ; *Am. Home Assur. Co. v. Societe Commerciale Toutelectric* (2002) 104 CA4th 406, 426, 128 CR2d 430] .



Cross Reference:

Discussion of blocking statutes, see 14.24.

14.06[6] If California Court Orders Production Under Code of Civil Procedure, Foreign Party Must Comply or Face Sanctions. If a California court orders production of the ESI over the objections of the foreign party, the foreign party must choose. Either it must comply with the California court's order, and the litigation proceeds, or it must choose to comply with its foreign obligations, and refuse to produce the ESI. A party that refuses to produce discovery in a U.S. court when ordered to do so faces the likelihood of sanctions [see *Richmark Corp. v. Timber Falling Consultants* (9th Cir. 1992) 959 F2d 1468 (making an *Aerospatiale* comity analysis in matter of sanctions against a mainland Chinese corporation)]. The court should take into account the importance of the missing discovery, and the likelihood of actual enforcement by the foreign government when considering the level of sanctions to impose [see, e.g., *Societe Internationale Pour Participations Industrielles v. Rogers* (1958) 357 US 197, 78 S Ct 1087, 2 L Ed2d 1255 (lower court's order for terminating sanctions reversed and case remanded on the grounds that threatened foreign criminal prosecution should have been given greater consideration as an excuse for non-production.); *US v. Vetco* (9th

Cir 1981) 691 F2d 1281 (monetary sanctions upheld as Swiss government had not moved to order compliance with local law; complying with IRS summons even though its attorneys argued that to fulfill its obligations under U.S. law would violate Swiss law)].



112 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
II. ANALYZING APPLICABLE CALIFORNIA LAW REGARDING DISCOVERY OF ESI RESIDING ABROAD

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.07

AUTHOR: Diane E. Barry, Esq.

14.07 Jurisdiction Must Be Obtained.

14.07[1] Jurisdiction Over Foreign Person in California Court Requires Appropriate Service of Process and Sufficient Minimum Contacts. In order to obtain jurisdiction over a foreign person or corporation, the person must be served using one of the methods approved of in the Code of Civil Procedure, and they must have sufficient minimum contacts with the State of California. There must be both minimum contacts and proper service.

If the foreign person or corporation resides abroad, jurisdiction may exist in California, but it will be necessary to serve the party abroad as well. This must be done using a method that both meets the requirements of the California Code of Civil Procedure, and is permissible in the foreign jurisdiction. The Hague Convention for Service [*see* 14.07[2][d]] and the Inter-American Convention for Letters Rogatory [*see* 14.07[2][c], 14.17[3]] both provide acceptable methods for service in the signatory countries.

Even if the foreign person can be served in California, it is often desirable to serve them abroad in a manner acceptable in the relevant foreign jurisdiction. If counsel needs to obtain ESI or other evidence located in the foreign nation, or if counsel wishes to enforce a judgment there, if the party was served in a manner that is acceptable to the foreign jurisdiction there will be fewer questions or hesitations about providing later requested judicial assistance.

14.07[2] Party Seeking Discovery Must Obtain Service of Process on a Foreign Person or Corporation.

14.07[2][a] Usual Methods Apply for Service Within California. If service can be made inside the State of California, any of the usual methods of service authorized in the CCP can be used [CCP §§ 413.10(a) (service outside state or country); 415.10 (personal service); 416.90 (substituted service)].

If a foreign corporation has a regular place of business in the State of California, or a substantially owned subsidiary with a regular place of business in the State of California, service can be made in the State of California rather than at the foreign offices of the corporation [*see Volkswagenwerk Aktiengesellschaft v. Schlunk* (1988) 486 US 694, 706-708, 108 S Ct 2104, 100 L Ed2d 722 (upholding jurisdiction of Illinois court over foreign corporation when service was made in Illinois on a domestic subsidiary of the foreign corporation); *Yamaha Motor Co v. Sup. Ct.* (2009) 174 CA4th 264, 94 CR3d 494 (foreign corporation could be served through its California subsidiary pursuant to the Code of

Civil Procedure rather than abroad pursuant to the Hague Convention for Service).]



Cross References:

California Forms of Pleading & Practice, Ch. 518, Service of Summons and Papers (Matthew Bender).

General Discussion of Service of Process, Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure, Chapter 8, Service of Summons.

14.07[2][b] Service Outside California but Inside United States Can Be Made Under Law of California or Other State. An individual or corporate person located outside of California, but still inside the United States, can be served either in accordance with the sections regarding service of process in the Code of Civil Procedure or as authorized by the laws of the state where the person is served [CCP § 413.10(b)].

14.07[2][c] Choices Exist for Service Outside of the United States. The Code of Civil Procedure authorizes various choices for how to serve a person located outside of the United States. Under the terms of the Code of Civil Procedure, use of the Hague Convention for the Service Abroad of Judicial and Extrajudicial Documents ("Hague Convention for Service") is permissive rather than required [CCP § 413.10(c)]. Case law, however, holds that the Hague Convention for Service preempts state laws regarding service of process outside of the United States, and is binding on the states. The Hague Convention for Service is a treaty ratified by the United States, and therefore is part of the law of this country. Under the *Supremacy Clause of the U.S. Constitution*, the Hague Convention for Service therefore preempts inconsistent methods of service prescribed by state law in all cases to which it applies [US Const art VI, cl 2; *Volkswagenwerk Aktiengesellschaft v. Schlunk* (1988) 486 US 694, 699, 108 S Ct 2104, 100 L Ed2d 722; *Kott v. Superior Court* (1996) 45 CA4th 1126, 1133, 53 CR2d 215]. In addition, CCP § 413.10 specifically states that it is subject to the Hague Convention [CCP § 413.10(c)].

Compliance with the Hague Convention for the Service is mandatory only when service is being made in a signatory country. A current list of signatories is available through the official Hague Convention website, located at http://hcch.e-vision.nl/index_en.php?act=conventions.status&cid=17. A list with helpful notes is also maintained by the U.S. Marshals Service at http://www.usmarshals.gov/process/hague_service.htm.

Failure to comply with the Hague Convention for Service when it is applicable renders service null and void, even if the defendant had actual notice of the lawsuit [*Floveyor Int'l, Ltd. v. Superior Court* (1997) 59 CA4th 789, 69 CR2d 457].



Cross Reference:

The full text of the Hague Convention for Service is available on lexis.com at 1969 UST LEXIS 152, or the International Agreements volume of the United States Code Service.



Strategic Points:

- The Hague Convention for Service should be used when serving a foreign corporation, even if there are options for service of process under the Code of Civil Procedure inside California or the United States.
- Unlike the discovery-related agreements of the Hague Convention, addressed in Sections 14.08-14.13, the rules for service of process are not difficult to comply with, as long as there is a known address where the foreign party can be served (service by mail is not acceptable in many foreign jurisdictions).

- If counsel needs to take discovery outside of the United States, or enforce a judgment outside of the United States, no other signatory country can quibble that service on the discovery target or judgment debtor was not properly performed [see Inter-American Judicial Committee, Report on Uniformity of Legislation on International Cooperation in Judicial Procedures (1952), 30)].
- Service in compliance with the Hague Convention is acceptable almost everywhere.
- Like ordinary service of process, there are companies that specialize in Hague Convention compliant service of process.

14.07[2][d] Procedure for Service of Process Under Hague Convention. Every signatory nation is required to designate a Central Authority to process service requests [Hague Convention on Service Abroad, art 2]. The court with jurisdiction over the case must order the service to be made pursuant to the Hague Convention, and issue an official request for service using the forms required under the Convention for service [Hague Convention on Service Abroad, art 2]. Service documents then must be provided to an official Central Authority of the receiving nation, which, in turn, sees to it that the papers are served in accordance with local requirements. If the requesting nation has a need for use of a particular method, it can request that that method be used. The receiving Central Authority will use requested methods unless domestic law prohibits [Hague Convention on Service Abroad, art 5]. If there are problems preventing service, the Central Authority is required to "promptly" inform the applicant and specify the problems [Hague Convention on Service Abroad, art 4]. Once service has been accomplished, the Central Authority of the receiving nation sends back a certificate of service using forms designated by the Convention [Hague Convention on Service Abroad, art 6].

Forms can be presented in French or English, the default acceptable languages of the Hague Convention, unless local law requires translation into the national language of the receiving nation.

Strategic Points:



- Although the Hague Convention permits default use of English or French, it is good practice to have the papers translated into the language of the receiving nation. Local courts and authorities are more likely to process more quickly if the papers are understandable. Furthermore, if there is ever a question of whether or not the papers provided or were intended to provide actual notice, there will be fewer arguments if the papers were sent in the local language. The expenses of hiring a certified court translator are much less than the costs of defending a law and motion challenge to the papers later on.
- A list of Central Authorities is maintained at the official website for the Hague Convention at http://hcch.e-vision.nl/index_en.php?act=conventions.authorities&cid=17.



Cross References:

Forms that must be issued by the court to request service abroad under the Hague Convention for Service, see 14.32-14.33.

Discussion of requirements for service under the Hague Convention for the Service of Abroad of Judicial and Extrajudicial Documents, *Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure*, Ch. 8, *Service of Summons* § 8.14.

Example--Hague Convention for Service:

Balcom v. Hiller (1996) 46 CA4th 1758, 54 CR2d 536 involved a suit in California state court for misappropriation of funds. The defendant was served in Great Britain in accordance with the Hague Convention for Service. The plaintiff successfully moved for a default judgment. The defendant attacked the judgment for lack of personal jurisdiction, and for failure to serve the complaint in accordance with the requirements of the Hague Convention for Service. The appellate court upheld the default judgment, holding that service had been valid under the requirements of the Hague Convention, as service had been made in accordance with the law of Great Britain, the receiving nation.

14.07[3] Jurisdiction in California Court Requires Minimum Contacts Analysis. A California court can only exercise personal jurisdiction over a foreign defendant if the defendant has certain minimum contacts with the forum state so that maintenance of the suit does not offend traditional notions of fair play and substantial justice [*International Shoe Co. v. Washington* (1945) 326 US 310, 316, 66 S Ct 154, 90 L Ed 95 ; *Pavlovich v. Superior Court* (2002) 29 C4th 262, 268, 127 CR2d 329, 58 P3d 2] . The California long-arm statute provides: "[a] court of this state may exercise jurisdiction on any basis not inconsistent with the Constitution of this state or of the United States" [CCP § 410.10]. When addressing the question of whether a particular exercise of personal jurisdiction comports with constitutional due process, the central inquiry is whether the defendant purposefully established minimum contacts in the forum state [*Burger King Corp. v. Rudzewicz* (1985) 471 US 462, 474, 105 S Ct 2174, 85 L Ed2d 528 ; see also *World-Wide Volkswagen Corp. v. Woodson* (1980) 444 US 286, 291, 100 S Ct 559, 62 L Ed2d 490] . The rule applies to individual defendants as well as to corporate defendants [*Arnesen v. Raymond Lee Org., Inc.* (1973) 31 CA3d 991, 996, 107 CR 744] .

Example--Proper Hague Convention Service but No Minimum Contacts:

In *Floveyor International v. Sup Ct* (1997) 59 CA 4th 789, 69 CR2d 457 , a California corporation sued a British corporation and properly arranged service in accordance with the Hague Convention for Service. The British corporation moved to quash, on grounds of lack of personal jurisdiction in California. The motion was granted as the record was "devoid of any evidence" that the British corporation had contacts with California.

 Cross Reference:

General discussion of minimum contacts analysis, see Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure, Ch. 9, Motions to Quash and Other Objections to Personal Jurisdiction



113 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions

III. CONDUCTING FOREIGN E-DISCOVERY USING THE HAGUE CONVENTION

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.08

AUTHOR: Diane E. Barry, Esq.

14.08 CHECKLIST: Conducting Foreign E-Discovery Using the Hague Convention.

☐ Is target ESI physically located outside of United States, its territories, and insular possessions?

Authority:

The Hague Convention for Evidence (requests are from one contracting state to another contracting state, to request testimony or materials located in the receiving state)

Discussion:

See 14.11

☐ Is nation where target ESI is physically located a signatory to Hague Convention on taking of Evidence Abroad in Civil or Commercial Matters?

Authority:

The Hague Convention for Evidence, Article 1 (requests are only authorized between contracting states), Article 38 (Convention enters into effect after ratification by the signatory state), Article 39 (additional nations may adopt/accede to the Convention at a later date.)]

Discussion:

See 14.11

Forms:

See 14.32-14.33

☐ Does counsel know address where custodian of ESI is located in Hague Convention contracting state?

Authority:

The Hague Convention for Evidence, Article 1 (requests are only authorized between contracting states), Article 3 (information to be specified in a Letter of request)

Discussion:

See 14.18[2] (letters rogatory)

Forms:

See 14.32-14.33

☐ Has nation where target ESI is physically located stated an exception to Hague Convention on Taking of Evidence Abroad in Civil or Commercial Matters that would impede production of desired ESI?

Authority:

The Hague Convention for Evidence, Article 12 (contracting states may refuse to execute a letter of request if it considers that its sovereignty or security would be prejudiced); Article 23 (contracting states may, at the time of signing or acceding, declare that they will not support the use of letter of request for pre-trial discovery as that term is used in common law countries)

Discussion:

See 14.11[4], 14.13[1]

Forms:

See 14.32-14.33

☐ Does nation where desired ESI is physically located have a blocking statute or other legal impediment to U.S.-style pre-trial discovery that can be overcome by use of letters of request issued pursuant to Hague Convention on taking of Evidence Abroad in Civil or Commercial Matters?

Authority:

The Hague Convention for Evidence, Article 12 (contracting states may refuse to execute a letter of request if it considers that its sovereignty or security would be prejudiced), Article 23 (contracting state may file reservation refusing to execute letter of request that seeks pre-trial discovery); *Societe Nationale Industrielle Aerospatiale v. US Dist Ct* (1987) 482 US 522, 107 S Ct 2542, 96 L Ed2d 461 (French ministry offered to withdraw opposition to depositions if they were noticed via letter of request)

Discussion:

See 14.24

Forms:

See 14.32-14.33



114 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
 III. CONDUCTING FOREIGN E-DISCOVERY USING THE HAGUE CONVENTION

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.09

AUTHOR: Diane E. Barry, Esq.

14.09 Objective and Strategy.

The Hague Convention on Taking of Evidence Abroad in Civil or Commercial Matters ("Hague Convention for Evidence") provides vehicles for taking both documentary and testimonial evidence. Attorneys who find it necessary to obtain ESI located in a nation subject to the Convention may use the procedures described in this part to obtain that evidence.



Strategic Point:

Foreign parties often prefer to supply ESI under a Hague Convention on Taking of Evidence letter of request rather than a California discovery request. This preference sometimes can be used as a negotiating point among the parties [see 14.05[1]].

Consider:

Each Hague Convention (for service, for taking of evidence, and so on) has a separate list of signatories--those nations that are officially willing to abide by that particular Hague Convention. The signatories differ from convention to convention. Although most of the EU nations are signatories to the Hague Convention for the Taking of Evidence, many nations outside the EU also have ratified the treaty. For example, Venezuela, the Ukraine, and Australia are all signatories to the Hague Convention on Taking of Evidence. In addition, each signatory nation is permitted to file exceptions and explanations, and most do. For the most current and complete information on whether the nation where the ESI is physically located is indeed a signatory to the Hague Convention for the Taking of Evidence, counsel should check the current list of signatories, and the status table showing any reservations they may have filed. The official website for the Hague Conventions keeps a current list of the nations signatory to each of the various Hague treaties. The current list of the Contracting States for the Hague Convention for the Taking of Evidence, and all filed reservations and explanations, is located at http://hcch.e-vision.nl/index_en.php?act=conventions.status&cid=82 (see the "status table" for the convention).



115 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
III. CONDUCTING FOREIGN E-DISCOVERY USING THE HAGUE CONVENTION

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.10

AUTHOR: Diane E. Barry, Esq.

14.10 Treaties and Other Agreements Set Scope of International Discovery.

14.10[1] Treaties Define Scope of International Discovery. When foreign nationals are parties to California litigation, they are subject in California to California's authority and California's rules [see 14.07, 14.05]. However, when ESI is located outside California, or further, outside of the reach of the government of the United States, attempts to obtain it confront the sovereign authority of another nation, which rightfully seeks to protect its own citizens against foreign intrusion, and to regulate the interaction of its citizens with any foreign judicial process.

Essentially, one sovereign cannot order the subjects of another sovereign to perform any act within the latter's territory. The sovereign seeking performance of the act must "ask nicely" of the foreign sovereign, and if the request is acceptable to the foreign sovereign, the sovereign seeking performance may proceed. In practice, this means that the United States diplomatic corps works to set up international agreements to assist litigants in obtaining the evidentiary materials they need. Agreements can be formal, as in a treaty or convention, or they can be informal, such as those available by communications through diplomatic channels.

Treaties are pre-existing agreements between sovereigns. Treaties that are ratified by the United States Senate and signed by our President enter the laws of the United States [U.S. Const., Article VI, *cl. 2*; *Article III*, § 2, *cl. 1*]. United States citizens are bound by them, and can make use of them.

Distinguish--Letters Rogatory:

If there is no such pre-existing treaty or agreement, there can still be agreement in the international community on how to "ask nicely" for evidence, and how to address a nation that has no pre-existing obligation to heed a request originating in the United States. Letters rogatory may be used for this purpose.

➡ Cross Reference:

Detailed discussion of use of letters rogatory, see 14.14-14.19.

14.10[2] Hague Convention for Evidence Can Be Used to Obtain ESI. The Hague Convention for Evidence is a treaty that permits litigants to obtain ESI, paper documents, and the testimony of witnesses, which reside abroad. This is

accomplished through permissive use of the judicial and sovereign authority of the hosting foreign nation [Hague Convention for Evidence, Preamble and Article 1]. The Hague Convention for Evidence is binding upon all signatory nations [see 14.11]. Signatories agree to provide each other with the listed kinds of assistance in obtaining cross-border evidence for use in civil and commercial disputes, provided it is asked for in the agreed upon ways.

 Cross References:

Issuance and execution of letters of request, Hague Convention for Evidence, Articles 1-14.

Circumstances under which receiving contracting state may refuse to execute a particular letter of request, Hague Convention for Evidence, Articles 15, 12.

Authority for contracting states to file general refusal to execute any letter of request that seeks common law style pre-trial discovery, Hague Convention for Evidence, Article 23.

Contracting state required to compel appearance and testimony of witnesses and production of documents, Hague Convention for Evidence, Article 10.

Authority for contracting state to excuse the testimony of witness if such testimony would be considered privileged either under domestic laws of receiving state or under laws of requesting state, Hague Convention for Evidence, Article 11.



116 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions

III. CONDUCTING FOREIGN E-DISCOVERY USING THE HAGUE CONVENTION

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.11

AUTHOR: Diane E. Barry, Esq.

14.11 Hague Convention on Taking of Evidence Abroad in Civil or Commercial Matters--General Principles and Structure.

14.11[1] Hague Convention Was Intended to Assist Transfer of Evidence Materials Between Civil Law and Common Law Nations. Diplomatic and political differences aside, one of the most difficult points of obtaining evidence abroad stems from the differing legal philosophies regarding the taking of evidence which exist between civil law and common law states.

In common law states, the taking of evidence in civil litigation generally is a private matter. Requests are issued by private citizens--party litigants and their counsel. ESI, documents, and testimony are all taken and exchanged privately, usually outside of the presence of a judge or other government official.

In civil law nations, in contrast, the taking of evidence is a judicial and government prerogative. Judges take testimony. Private citizens do not. Therefore, civil law nations view common law discovery requests as an infringement on sovereign functions [discussion on Civil Law and Common Law issues, Report of the U.S. Delegation to the Hague Convention]. The Hague Convention on Evidence was intended to create methods that both systems could tolerate [*Societe Nationale Industrielle Aerospatiale v. US Dist Ct (1987) 482 US 522, 529, 107 S Ct 2542, 96 L Ed2d 461* ; Report of United States Delegation to Eleventh Session of Hague Conference on Private International Law (discussion of problems of sovereign infringement caused by common law discovery practices in civil law nations)].

14.11[2] Letters of Request Under Hague Convention for Evidence Are Preferable to Letters Rogatory If Discovery Under California Code of Civil Procedure Is Not Available. The Code of Civil Procedure is preferable for conducting outright pre-trial discovery [see 14.05[1]]. The access to ESI, documents and witnesses authorized by the Code of Civil Procedure is much broader than that available either under the Hague Convention for Evidence or through letters rogatory.



Cross Reference:

Advantages and use of Code of Civil Procedure for e-discovery, see 14.05, 14.11[4]

However, as between the Hague Convention for Evidence and letters rogatory, the Hague Convention is preferable. The Hague Convention's letters of request are considerably broader in function than letters rogatory and have stronger enforcement provisions [*Hague Convention for Evidence, Articles Volkswagenwerk Aktiengesellschaft v. Superior Court* (1981) 123 CA3d 840, 853, 176 CR 874 (citing Report of the U.S. Delegation to the Hague Convention, p. 807)].

➡ **Cross Reference:**

Use of letters rogatory, see 14.14-14.19.

14.11[3] Application Limited to Hague Convention Signers. The Hague Convention treaty refers to signatory nations as "contracting states." The agreement under the treaty is that requests can be made by a contracting state, to a contracting state [Hague Convention for Evidence, Article 1; approved forms for letters of request for documents or depositions under the Hague Convention].

➡ **Cross Reference:**

Hague Convention signatories, see 14.11[3];
http://www.hcch.net/index_en.php?act=conventions.text&cid=82.

14.11[4] Availability of Pre-Trial Discovery Is Limited in Many Hague Convention Nations.

14.11[4][a] Hague Convention for Evidence Permits Contracting States to File Reservations Limiting Pre-Trial Discovery. Article 23 of the Hague Convention for Evidence specifically authorizes contracting states to file reservations against accepting letters of request which seek pre-trial discovery [Hague Convention for Evidence, Article 23]. Most signatory states have filed reservations or explanatory declarations or both. A list of the countries that have filed reservations and declarations can be found in the Hague Convention for Evidence Status Table maintained by the official Hague Convention website [http://www.hcch.net/index_en.php?act=conventions.status&cid=82].

Examples--Hague Convention for Evidence Reservations and Declarations:

- France, Germany, India, Italy, and the United Kingdom have all filed reservations refusing to recognize letters of request that seek pre-trial discovery, as authorized by Hague Convention for Evidence, Article 23.
- The United States has filed a declaration explaining that it will accept a letter of request in Spanish, but only for service in Puerto Rico, and that a letter of request filed in French will be accepted, but will take longer to process than those filed in English.

Example--Foreign Court Restrictions on U.S.-Style Pre-Trial Discovery:

In *Rio Tinto Zinc Corp. v. Westinghouse Elec. Corp.* (1978) AC 547, suit was filed in United States courts for breach of contract based on failure to construct two nuclear power stations. Letters rogatory, which were converted to letters of request under the Hague Convention for Evidence, were issued for both testimony and documents. The document request went up through the British courts to the House of Lords. The House of Lords upheld severely limited documentary discovery, noting "a strict attitude is to be taken by English courts in giving effect to foreign requests for the production of documents by a non-party witness." It was also noted that the lower court had properly limited the documentary discovery to those allowed by English law, and that the court should only require production of "[p]articular documents specified in the order as being documents appearing to the court making the order to be, or to be likely to be, in his possession, custody or power."

14.11[4][b] Letter of Request Must Relate to Pending or Contemplated Judicial Proceeding. Letters of request

can be used to obtain evidence only for a judicial proceeding, either one already commenced, or one contemplated [Hague Convention for Evidence, Art. 1].

14.11[5] Costs of Letter of Request Procedure Should Be Evaluated. Most nations do not charge for execution of letters of request. However, if the executing country incurs expenses for fees paid to "experts and interpreters," the executing country may seek reimbursement.

Examples:

- If the papers were supposed to be filed in a particular language, and they were not [*see 14.12[3][d]*], the executing country can either send them back as non-compliant, or may choose instead to pay to have them translated and charge back a translation fee [Hague Convention for Evidence, Article 14].
- The Convention also concedes that some nations may be constitutionally required to charge for the judicial costs of the services provided [Hague Convention for Evidence, Art. 16].

The United States Department of State publishes information on the usual practices in the various nations signatory to the Hague Convention.



117 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
 III. CONDUCTING FOREIGN E-DISCOVERY USING THE HAGUE CONVENTION

*1-14 MB Practice Guide: CA E-Discovery and Evidence 14.12***AUTHOR:** Diane E. Barry, Esq.**14.12 Letter of Request Must Be Sent to Foreign Nation.**

14.12[1] Party Seeking Discovery Must Have California Court Issue Letter of Request. Letters of request must be issued by a judicial authority [Hague Convention for Evidence, Art. 1]. Thus, a letter of request in a California judicial proceeding must originate with the court, not the litigants as in California. In practice, however, the litigant seeking the discovery prepares the necessary papers for the California court's signature and issuance. [see 14.12[3]].

14.12[2] Party Seeking Discovery Must Prepare and File Motion to Issue Letter of Request in California Court. A letter of request to obtain ESI must be issued by the court in California to the proper receiving authority in the nation where the ESI is physically located. The requesting party must make a motion requesting that the California court issue the letter of request. If the matter has been discussed with opposing counsel first, and agreement on this point reached, the motion can be made as an oral motion in open court during a hearing or discovery conference. All counsel can agree on the record. If no agreement has been reached on this point beforehand, a written motion can be filed either ex parte or under the ordinary law and motion rules for noticed motions.

**Cross Reference:**

General discussion of law and motion procedure, see Matthew Bender(R) Practice Guide: Pretrial Civil Procedure, Ch. 26, Law and Motion Procedure.

**Strategic Points:**

- If the judge is not familiar with the Hague Convention or the general requirements for foreign discovery, it may be best to file a written motion giving some explanation of these points. If there is no disagreement among counsel, the papers can be filed with a stipulation to shorten time and a statement of non-opposition.
- In some cases, counsel for the custodian of the foreign ESI will agree to respond to the discovery if it

is issued in the form of a Hague Convention letter of request rather than as a U.S. discovery [see 14.05[1]]. In such cases, the motion requesting the issuance of the letter of request often is not contested. The heated contentions in this area most frequently occur beforehand, when the discovery target has asked the requesting counsel to use the Hague Convention rather than the Code of Civil Procedure to effectuate the discovery. Once agreement has been reached to use letters of request, the actual issuance can be much less contentious.

- If counsel have not reached an agreement, counsel for the discovery target should consider using an opposition to the motion to issue letters of request as a place to begin presenting objections to the scope of the request. For example, an opposition brief can object to the issuance on the grounds that responding to such a request will be monetarily burdensome, that the proposed letter of request is in actuality a pre-trial "fishing expedition" that is not authorized by the Hague Convention, and/or that the letters request items that cannot be produced without violation of foreign law. This can assist in negotiations with foreign ministries: such an opposition shows that the ESI custodian is putting up a vigorous defense of its foreign obligations. It also can provide the California court with a preview of problems to come [see 14.23, 14.24].

- Even if the initial motion to issue the letter of request is unopposed, it may still bog down later in the process. Objections to the scope of the letter of request often arise in the foreign jurisdiction rather than in the California court. See Part V of this chapter [see 14.20-14.24], dealing with foreign barriers to discovery. Briefly, the central authority that receives the letter of request can examine the letter for compliance with the Hague Convention for Taking of Evidence. If the letter of request violates the convention, the local ministry can refuse to enforce it, or can unilaterally decide to narrow the scope to the bounds it considers legal. The foreign discovery target can also make objections to the scope after receiving the letter of request on the basis that compliance with the request will require them to violate local law. The objections of the discovery target can be made either in California court, or in a court of the nation where the letter of request was served, or both.

14.12[3] Party Seeking Discovery Must Prepare Form for Letter of Request.

14.12[3][a] Party Should Prepare Letter of Request Form for Court's Signature. The moving party also should fill out the form for the letter of request for document, and attach it to the motion so that it can be issued by the court or court clerk. The Hague Convention for Evidence has issued forms that must be used for letters of request.



Cross References:

Language requirements for letters of request, see 14.12[3][d].

Form, sample motion for issuance of letters of request, see 14.30.

Official forms for letters of request, see Forms 14.32, 14.33.



Warning:

The forms should not be altered, except as permitted in the instructions. Some paragraphs are alternatives, and the unused items can be removed.

14.12[3][b] ESI Should Be Described As Specifically As Possible to Maximize Possibility of Success. Most of the Hague Convention for Evidence signatory states have filed reservations under Article 23 stating that they will not execute letters of request that seek U.S.-style pre-trial discovery [see 14.11[4]]. Even without an Article 23 reservation, most civil law nations will not comply with a letter of request that seeks to find out whether or not particular categories of documents exist and are in the possession of the letter recipient. Their own laws do not support this kind of demand

and indeed, often block compliance with such demands [see 14.24 (blocking statutes)].

This means that letters of request are weakest, and the most likely to meet refusal, when they seek to find out if particular documents exist at all, or to get a general roadmap of what kind of documents are in the recipient's possession. They are strongest when the letter of request can specify either individual documents, or categories of documents that are likely to be in the possession of the letter recipient [see *Rio Tinto Zinc Corp. v. Westinghouse Elec. Corp.* (1978) AC 547 (House of Lords case in which U.S. letters of request were severely limited in scope to avoid pre-trial discovery under the laws of the United Kingdom)].

14.12[3][c] Letter of Request May Ask That Particular Procedures Be Followed. The letter of request can ask that particular procedures be followed. Such procedural requests are not binding on the foreign nation [Hague Convention for Evidence, Art. 9; see 14.13[3]]. In practice, this section is used to request U.S.-style procedures when they are desirable, and not in contravention of local law.

In the case of ESI, if particular procedures are needed so that the evidence will be usable in the recipient court system, they should be specified. For example, it is advisable to request a forensically sound collection method by a specialized technician having certain types of certifications or qualifications (EnCe, CCE, CISSP, etc.). The technician should be instructed to provide chain-of-custody documentation so that the evidence can be entered into evidence [see *Lorraine v. Markel (D MD 2007) 241 FRD 534*]. Counsel should consider locating local technicians or companies who can provide the services, and offering them for use, at the parties' expense. If the particular matter has other requirements as to delivery format or otherwise, they should be specified in the letter.



Warning:

If the requirements are too onerous, the local authority can ignore them completely. The requirements should be simple and easy to understand and comply with. Counsel may need to make do with less than the usual items obtained by U.S.-based technicians. Such a procedure should be discussed with opposing counsel and the court before spending time and money on such an ESI production. It is best to have a stipulation or court order stating that the ESI obtained under the letter of request will be deemed admissible.

14.12[3][d] Letter of Request Must Meet Hague Convention Language Requirements. A letter of request may be filed in accordance with either of the following language requirements [Hague Convention for Evidence, Art. 4.]:

- It is always acceptable to file letters of request in the official language of the nation to which letters of request are being sent, or to send an accompanying translation into that language. If a translation is sent, it must be certified as correct either by a diplomatic officer, a consular agent, or a sworn translator.
- Alternatively, all documents may be submitted in French or English, unless the receiving nation has specifically filed a reservation on this point.



Strategic Point:

A list of the countries that have filed reservations can be found in the Hague Convention for Evidence Status Table maintained by the official Hague Convention website:
http://www.hcch.net/index_en.php?act=conventions.status&cid=82. Counsel should consult this list before preparing a letter of request for signature by a California court.

14.12[4] California Court Forwards Letter of Request to Designated Central Authority of Foreign Nation.

After the California court has issued the letter of request, the court will forward it to the central authority for the nation where the ESI resides.

The letters must be sent from the California court to the Central Authority of the receiving nation. Counsel cannot mail them or otherwise convey them. However, it is frequently the practice for counsel to prepare the mailing materials for the court clerk, which may help expedite processing and avoid transmission errors. Counsel should contact the clerk of the California court to determine the clerk's usual practice and preferences.

Consider:

Any response or correspondence from the other country's courts will be sent to the California court or court clerk, not to counsel.



Strategic Point:

Each Hague Convention contracting state designates a central authority where letters of request should be filed [Hague Convention for Evidence, Art. 2]. A current list of Hague Convention central authorities is maintained on the official website for the Convention [see http://www.hcch.net/index_en.php?act=conventions.authorities&cid=82]. The U.S. Department of State also maintains a list of central authority offices, together with helpful notes [see http://travel.state.gov/law/info/judicial/judicial_689.html].



118 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions

III. CONDUCTING FOREIGN E-DISCOVERY USING THE HAGUE CONVENTION

*1-14 MB Practice Guide: CA E-Discovery and Evidence 14.13***AUTHOR:** Diane E. Barry, Esq.**14.13 Foreign Nation Will Act on Letter of Request.**

14.13[1] Central Authority May Raise Objections to Letter and Must Notify California Authority of Objections. The central authority can refuse to serve the letter of request if it violates the Hague Convention generally, or if it violates an exception to the Convention filed by the receiving nation [Hague Convention on Taking Evidence, Arts. 12, 23]. In extreme cases, it can refuse if it considers that the letter of request infringes upon its "sovereignty or security" [Hague Convention on Taking Evidence, Arts. 12, 23].

If the receiving Central Authority believes that the letter of request does not comply with the Hague Convention or one of the reservations filed by the receiving nation, the central authority must "promptly" inform the judicial authority that sent the request, stating the nature of the objections [Hague Convention for Evidence, Art. 5]. A contracting state can refuse to execute a properly executed and delivered letter of request only if the receiving state believes that its "sovereignty or security" would be prejudiced by enforcement [Hague Convention for Evidence, Art. 5].

Strategic Points--Responding to Objections from Central Authority:

- If the objections are purely technical, they can be dealt with by revising the letter. The most difficult problem to overcome is an objection that the letter of request is demanding pre-trial discovery. Most Hague Convention signatory nations have filed exceptions to this use of the Hague Convention [see 14.11[1],[4]]. The more extensive the letter of request is, the more likely this is to happen. It may be necessary to provide the central authority with an explanation of why the materials sought are known to be, or are reasonably likely to be, in the possession of the custodian named in the letter. If the ESI custodian has agreed to the discovery, the custodian can also let the authority know that it understands what ESI is being requested and stands ready to comply once the letter of request is served (this is easiest to negotiate with parties).

- Local counsel in the foreign jurisdiction can be of tremendous assistance in negotiating such items

with a foreign central or local enforcing authority and finding out what would allay local hostility to the letter of request.

- It may also be necessary to accept a central authority's decision to limit the scope of the letter of request, and to attempt to obtain the ESI from other sources or through other means.

14.13[2] Central Authority Will Forward Letters of Request to Appropriate Local Authority in Foreign Nation for Execution. The central authority, after determining that the letter of request meets Hague Convention requirements, will then forward the letter of request to the local authority within the foreign nation that is competent to carry out the particular commission (taking testimony, receiving production of ESI or documents, etc.) [Hague Convention for Evidence, Art. 2].



Timing:

The letter of request must be executed "expeditiously," and if it is sent to the wrong domestic authority for execution, the letter of request must be re-routed "forthwith" to an authority that can execute it [Hague Convention for Evidence, Arts. 6, 9]. In practice, the timing can differ greatly across jurisdictions. If the nation enforcing the letter of request is one that regularly receives and processes international requests, the timing is likely to be faster--a few months. If the enforcing nation or local authority has less experience in such matters, or if there is strong local hostility to the kind of request, the process can stretch out much longer.



Strategic Point:

The enforcing local authority may not be willing to discuss the letter of request with U.S. counsel. The letter of request is from one government to another government, and the local authority therefore may be unwilling to provide status reports to any requestor other than the local California court that issued the request. If the response is dragging on, counsel can try sending a polite request for an update. If it is ignored, counsel should ask the California court to make a polite request for an update. If it is ignored, or if the response is not sufficiently informative, counsel should then consider trying foreign informal measures. If the amount in controversy and the importance of the ESI merits, it can be worth the expense of working with counsel local to the foreign jurisdiction, who speaks the official language and is in touch with the local sensitivities and legal culture. Local counsel can speak informally with the local foreign authority and ask about the request. For example, the wording might need to be adjusted, or a technical resource paid for and set at their disposal. Local counsel can be better at discussing such items with a foreign ministry.

14.13[3] Receiving Nation Will Use Its Own Procedures, but Will Consider Procedural Requests. The executing judicial authority will use its own law, methods, and procedures [Hague Convention for Evidence, Art. 9]. However, other or additional procedures can be requested in the letter of request. If the requested procedures are not contrary to local law, and are not a practical barrier to execution, the local judicial authority will follow the procedures requested [Hague Convention for Evidence, Art. 9; *see 14.12[3][c]*].

14.13[4] Receiving Nation Must Enforce Letter of Request As It Would Similar Domestic Requests. The local authority is required to apply "appropriate measures of compulsion" and to the same extent used by local proceedings to obtain compliance with the letter of request [Hague Convention for Evidence, Art. 10]. In practice, the court will order a reluctant entity to comply, and can use such means as they have at their disposal to enforce their own orders. Local privileges will apply. For example, if there is a local privilege such as the Swiss banking secrecy acts, or local blocking statutes, the local court cannot require that the local entity break the local law to comply with the foreign letter of request. Local entities can object on this basis.

14.13[5] Requesting Authority Must Be Informed If Letter of Request Cannot Be Executed. If the local authority is not able to execute the request (for example, if the desired documents does not exist, or if the production is barred by local privilege or other legal barrier), the requesting authority will be informed immediately, and informed of the reasons why execution was not possible [Hague Convention for Evidence, Art. 13].

Consider:

Any response or correspondence from the other country's courts will be sent to the California court or court clerk, not to counsel.

14.13[6] Local Authority Will Enforce or Refuse to Comply With Letter of Request.

14.13[6][a] Local Authority Serves Letter of Request on ESI Custodian. After the central authority forwards the letter of request to the appropriate local authority, the local authority serves the letter of request on the custodian of the ESI under local procedures, and collects the response. If the custodian resists or ignores the letter of request, the local authority uses whatever coercive measures it usually uses for document requests to enforce the letter.

14.13[6][b] Custodian of ESI Can Object Under Local Law. Once served, the ESI custodian who receives the letter of request can object to it on the grounds that responding would require them to waive a valid privilege, or to otherwise violate local law. These objections can be raised in the foreign jurisdiction or in California, or both.

The foreign ESI custodian may be legally required to object to the discovery on the grounds that it would require them to violate local law [see 14.20-14.24]. A local ministry or other local foreign authority can also issue an order demanding that the ESI custodian not comply with the letter of request.



Strategic Point--Preferable for Requesting Party to Handle Objections in California Court:

Although the Hague Convention requires that a local authority use its coercive powers to enforce the letter of request, it need only do so to the extent that local law would apply coercion to enforce its own similar requests [Hague Convention on the Taking of Evidence, Art. 10]. A foreign authority is not likely to authorize coercion for an ESI production that violates its own laws. The best place to handle such objections is in the California court that issued the letter of request. If the ESI custodian is a party, and refuses to comply with the letter of request, the California court can issue local sanctions [see 14.03-14.07; 14.20-14.24].



119 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions

IV. CONDUCTING FOREIGN E-DISCOVERY USING LETTERS ROGATORY

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.14

AUTHOR: Diane E. Barry, Esq.

14.14 CHECKLIST: Conducting Foreign E-Discovery Using Letters Rogatory.

☐ Is it necessary to use letters rogatory to obtain production of ESI?

☐ Is desired ESI physically located outside United States, its territories, and insular possessions?

Authority:

CCP §§ 2026.010, 2027.010

Discussion:

See 14.10

☐ Is nation where desired ESI is physically located a Hague Convention for Evidence signatory?

Authority:

CCP §§ 2026.010, 2027.010; 23 UST 2555

Discussion:

See 14.11[3]

☐ Is nation where desired ESI is physically located a signatory to Inter-American Convention on Letters Rogatory?

Authority:

CCP §§ 2026.010, 2027.010; 14 ILM 339

Discussion:

See 14.17[3]

- ☐ Is a current address available for location where desired ESI is physically located, or for custodian of desired ESI?

Authority:

Second Inter-American Specialized Conference on Private International Law: Additional Protocol to the Inter-American Convention on Letters Rogatory, May 8, 1979; *18 ILM 1238*, Forms A & B

Discussion:

See *14.18[2]*

Form:

See *14.35*

- ☐ Would production of ESI breach any domestic laws or cultural norms of nation where ESI is physically located?

Authority:

14 ILM 339, Art. 17

Discussion:

See *14.19[4]*

- ☐ Consider obtaining assistance of counsel local to foreign jurisdiction to assist with drafting and foreign negotiations regarding letter rogatory.

Authority:

14 ILM 339, Arts. 13 and 17

Discussion:

See *14.16[1]*

- ☐ Contact foreign ESI custodian or counsel to negotiate a voluntary ESI production, if ESI custodian is willing to comply with a properly presented letter rogatory.

Authority:

14 ILM 339, Art. 3

Discussion:

See *14.19[5]*

- ☐ Contact U.S. State Department and discuss delivering letter rogatory to State Department for processing.

Authority:

14 ILM 339, Art. 4; *28 USC §1781(a), (b)*

Discussion:

See *14.19[2]*

- ☐ If letter rogatory will not be delivered to U.S. State Department, identify proper foreign authority to whom letter rogatory should be delivered.

Authority:

14 ILM 339, Art. 4

Discussion:

See 14.19[2]

- ☐ Identify any specialized procedures that may be required for collection and delivery of desired ESI in order for it to be usable in California proceeding.

Authority:

14 ILM 339, Art. 10

Discussion:

See 14.18[5]

Form:

See 14.30

- ☐ Prepare letter rogatory.

Authority:

Additional Protocol to the Inter-American Convention on Letters Rogatory, 18 ILM 1238 (1979), Art. 3

Discussion:

See 14.18

Form:

See 14.30

- ☐ Have letter rogatory and accompanying documentation translated by certified translator into official language of receiving nation.

Authority:

14 ILM 339, Art. 3(b); Additional Protocol to the Inter-American Convention on Letters Rogatory, 18 ILM 1238 (1979), Art. 3

Discussion:

See 14.18[3][a]

- ☐ Prepare and file notice of motion, motion, and proposed order, requesting court to issue letters rogatory.

Authority:

14 ILM 339, Art. 4

Discussion:

See 14.18[6]-[7], 14.19

Form:

See 14.30



120 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
IV. CONDUCTING FOREIGN E-DISCOVERY USING LETTERS ROGATORY

*1-14 MB Practice Guide: CA E-Discovery and Evidence 14.15***AUTHOR:** Diane E. Barry, Esq.**14.15 Objective and Strategy.**

Letters rogatory provide a vehicle to obtain production of ESI and other evidence when there is no treaty or other agreements between the United States and the nation where the evidence or witness resides. Letters rogatory request official assistance with various legal functions that, if performed without permission, would constitute an affront to or infringement of the receiving nation's sovereignty.

A letter rogatory is a formal request from a U.S. court to a court of a foreign jurisdiction requesting its judicial assistance in obtaining evidence for use in a matter before the U.S. court [22 *CFR* § 92.54 (letters rogatory defined); see *Volkswagenwerk v. Sup. Ct.* (1973) 33 *CA3d* 503, 507, 109 *CR* 219]. Letters rogatory can request almost any kind of judicial act, including service of process, taking of evidence, serving subpoenas, serving other legal notices, and the execution of a civil judgment [22 *CFR* § 92.54]. Letters rogatory usually require a statement of reciprocity--that the California court or the United States is willing to provide the same kind of assistance [see 22 *CFR* § 92.54 (letters rogatory defined)].

Consider:

Letters rogatory are a vehicle for comity among nations. One sovereign can use them to respectfully request assistance from another sovereign. The focus with a letter rogatory is that the nature of this transaction is a *request*. There are historical and treaty agreements as to the proper procedures for drafting and presenting a letter rogatory. However, unlike the Hague Convention, there is not necessarily any agreement by the receiving nation to speedily execute them, or to apply strong efforts or compulsion to obtain the items requested. The ability of U.S. litigants to obtain production of evidence through letters rogatory can depend on the current state of diplomatic relations with the receiving nation.

Strategic Points:

- For California litigants, letters rogatory should be the international production vehicle of last resort. They will not support a request anywhere near the scope of discovery under the Code of Civil Procedure, and they lack the reliability and enforcement strength found in letters of request under the Hague

Convention. If there are other routes to the materials needed, those routes should be considered first.

- Letters rogatory may need to be a choice if the nation where the ESI, documents or witness resides was once a Hague Convention signatory, but revolution or other similar change in government has occurred. The Convention requests that new governments confirm their intention to continue as a contracting state. During the pendency between the institution of such a new government and the filing of such a statement with the Convention, the state's willingness to execute Hague Convention requests can be in question. Letters rogatory are always available as an option in the place of a Hague Convention letter of request or request for service. However, because letters rogatory lack reliable structures for execution and enforcement, parties should try letters of request first, and see if they are honored. The U.S. Marshals Service maintains a list on its website showing the status of countries regarding the Hague Convention for Service [http://www.usmarshals.gov/process/hague_service.htm]. For example any country that has "achieved independence" and has not yet filed a declaration that it will continue to support to the Hague Convention for Service is in question.



121 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions

IV. CONDUCTING FOREIGN E-DISCOVERY USING LETTERS ROGATORY

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.16

AUTHOR: Diane E. Barry, Esq.

14.16 Counsel Should Research Judicial Resources Available to Assist With Letters Rogatory in Recipient Country.

14.16[1] Counsel Should Research Local Law and Judicial Attitudes. Counsel should research issues in the relevant country before requesting issuance of letters rogatory. Inquiry should include the following topics:

- Is the foreign country a signatory to an international treaty or convention relating to letters rogatory?
- What are the cultural and judicial attitudes towards the evidence being sought?
- What are the cultural and judicial attitudes towards various ways of gaining access?
- To whom should the letter rogatory be addressed, and how will it be delivered?

Strategic Points:



The first places to look are the website for the U.S. State Department, and, if relevant, the website for the Inter-American Convention on Letters Rogatory:

- The U.S. Department of State maintains a website describing the assistance available and local pitfalls in the listed nations [see http://www.travel.state.gov/law/info/judicial/judicial_2510.html].
- The Organization of American States (OAS) maintains a website with information on which nations are signatories to the Inter-American Convention on Letters Rogatory, and whether there is a Central Authority where letters rogatory can be filed in the first instance [see <http://www.oas.org/juridico/english/sigs/b-46.html>].

Example--Research on Receiving Nation's Resources and Attitudes:

Brazil is not a contracting nation under the Hague Convention for Evidence, but does accept and process letters rogatory. If the judicial act desired is service of process, the Inter-American Convention on Letters Rogatory can be used, and Brazil has identified a central authority to receive them. Although the United States has filed reservations against using the Inter-American Convention for purposes other than service of process, Brazil has not. Therefore, Brazil is apparently not adverse, in principle, to receiving letters rogatory for the purpose of obtaining ESI.

14.16[2] Counsel Should Consider Obtaining Assistance of Foreign Counsel. Letters rogatory are non-coercive. The nation must be willing to receive and process it; the recipient must be willing to respond. Local counsel can provide invaluable assistance in several ways.

- Local counsel can assist with the wording of the letter rogatory to avoid local sensitivities or illegalities.
- Local counsel can negotiate more easily with local authorities to gain acceptance of the letter rogatory, and to shepherd it through the process.
- Local counsel can negotiate compliance with the recipient of the letter rogatory.
- The involvement of local counsel manifests the parties' willingness to abide by local law and judicial process.



122 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
IV. CONDUCTING FOREIGN E-DISCOVERY USING LETTERS ROGATORY

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.17

AUTHOR: Diane E. Barry, Esq.

14.17 Letters Rogatory May Be Issued Pursuant to a Treaty or in Absence of Treaty.

14.17[1] Letters Rogatory Issued Under Treaty Generally Are Preferable. Various treaties among groups of nations formalize the practices of issuing, receiving, and executing letters rogatory. As issuance pursuant to a treaty provides more reliable process and results, that approach should be tried first if it is an available option.

14.17[2] Ordinary Letters Rogatory Can Be Issued If No Treaty or Convention Applies. Letters rogatory can always be issued as a polite request to any nation, even in the absence of any specific agreement. These are referred to as "ordinary letters rogatory." Ordinary letters rogatory, issued without any treaty or other agreement, are always an available choice. However, there are no agreements as to forms, execution, enforcement, response time, and so on. Although ordinary letters are always an available choice, they ought to be the final resort when all else has failed.

14.17[3] Party May Request ESI Under Inter-American Convention on Letters Rogatory If Foreign Nation Is a Signatory. The Inter-American Convention on Letters Rogatory ("IACLR") is a treaty among various nations in North, Central, and South America relating to the issuance, use, and recognition of letters rogatory among the signatory nations. The United States is a signatory to the convention, but has opted out of the portions of the IACLR that pertain to the taking of evidence [see IACLR, 14 ILM 339]. (However, the United States has not opted out of other judicial acts, such as service of process and recognition of judgments.)



Strategic Point--Lack of Reciprocity Does Not Necessarily Preclude Use of IACLR:

The U.S. decision to opt out of the IACLR sections for the taking of evidence casts some doubt on the ability of U.S. practitioners to use the convention to obtain ESI and other types of evidence under the treaty provisions. Ordinary letters rogatory practice requires that execution be reciprocal--"we'll execute yours if you promise to execute ours" [see 22 CFR § 92.54 (letters rogatory defined)]. However, the IACLR does not specifically require reciprocity among signatory nations. Therefore, counsel may wish to have letters rogatory issued under the IACLR first, and move to issuance of letters outside of the Convention if rebuffed by the foreign nation in question.

The official website to the Inter-American Convention on Letters Rogatory lists the signatory countries, reservations, and for each signatory nation identifies the central authority where letters rogatory can be filed [<http://www.oas.org/juridico/english/sigs/b-46.html>].

**Cross Reference:**

Text of IACLR, see *14 ILM 339* (available on [lexis.com](http://www.lexis.com))]



123 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
IV. CONDUCTING FOREIGN E-DISCOVERY USING LETTERS ROGATORY

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.18

AUTHOR: Diane E. Barry, Esq.

14.18 Preparation and Issuance of Letters Rogatory.

14.18[1] Letters Rogatory Must Be Issued by California Court. Like letters of request under the Hague Convention, letters rogatory must be issued from the California court with jurisdiction over the matter, to a government or judicial authority in the nation where the ESI, documents, or witness are located.

The letters rogatory must be sent from the California court to the appropriate authority of the receiving nation. Counsel cannot mail them. However, it is frequently the practice for counsel to prepare the mailing materials for the court clerk, which may help expedite processing and avoid transmission errors. Counsel should contact the clerk of the California court to determine the clerk's usual practice and preferences.

14.18[2] Counsel Should Consult Official Forms in Drafting Letters Rogatory. Before preparing letters rogatory, counsel should check the State Department's website, and the website of the relevant international organization, if any, to see if the receiving nation has posted or otherwise published its own form. If the request is being made under the IACLR, official forms have been adopted and must be used [*see Second Inter-American Specialized Conference on Private International Law: Additional Protocol to the Inter-American Convention on Letters Rogatory, May 8, 1979, 18 ILM 1238*].



Cross Reference:

Discussion of IACLR, see 14.17[3].

If there is no required form, the forms created by the Inter-American Convention on Letters Rogatory are a good place for counsel to start in drafting letters rogatory, even if the country in question is not a signatory to the IACLR.



Cross Reference:

Discussion of IACLR, see 14.17[3].

Forms:

See 14.34-14.36.

If counsel wishes to modify those forms, or draft an entirely new form, a letter rogatory must include at least the following items:

- **Request for International Judicial Assistance.** The letter rogatory should be addressed to "The Appropriate Judicial Authority of _____ [*name of nation*]." It should next state that this is a request for international judicial assistance and is being made in the interests of justice.
- **Statement Regarding Reciprocity and Costs.** Letters rogatory should include a statement from the requesting court expressing a willingness to provide similar assistance to judicial authorities of the receiving nation [see 22 CFR § 92.54 (letters rogatory defined)]. They should identify the person who will pay any necessary fees and costs associated with the judicial acts requested, and how the receiving judicial authority can contact that person.
- **Case Description.** Letters rogatory should include a brief description of the case, including that it is a civil matter (not criminal or administrative), identification of the parties, the nature of the claim, and relief being sought. The purpose is to enable the foreign court to understand the issues involved and the case basics.
- **Assistance Solicited.** The letter should state what kind of judicial assistance is being requested; for example, service of notices or other process; production of ESI; and/or other assistance.
- **Identity of Person Who Has Evidence Being Requested.** Letters rogatory should provide as much information as possible regarding the custodian of the evidence being requested. This should include the name, address, and any other identifiers, such as corporate title, of the person who is to be served, or who has the ESI or other evidence. Note that it is very important to provide a current address. If there is no address, the court will not know where to serve its domestic papers requesting/demanding that the witness or custodian appear and produce evidence. If adequate information is not provided, counsel is most likely to get either a response that states that the witness or custodian could not be found, or that service attempts were not successful.



Strategic Point:

It is preferable to contact the ESI custodian well before issuance to negotiate compliance with a letter rogatory. Local custodians appreciate hearing about a letter rogatory first before it simply arrives from the local judicial authority. In addition, the local ESI custodian knows that the local authority will not compel compliance. If the custodian is annoyed by the request or finds it burdensome, the letter rogatory will languish. Thus, counsel should ask the custodian what would assist him or her in sending the ESI requested. As part of the discussion with the custodian, it can be settled where to address the letter rogatory so that it is expected. If this is not possible, and the ESI custodian has a legal department, the letter rogatory should be addressed there.

14.18[3] Counsel Should Use Appropriate Language.

14.18[3][a] Letter Should Be Drafted in Language of the Receiving Nation. An ordinary letter rogatory, one issued not pursuant to a convention or other treaty agreement, is not a strong request. It is asking nicely of someone who is under no obligation whatsoever to provide the assistance requested. The foreign authority is not even obliged to provide information on how the request is or is not proceeding. In such a case, it is always best to send the letter rogatory in the official language of the nation where it is being presented. It is friendlier, and practically speaking, a letter that requires no translation is more likely to receive prompt and courteous attention. Letters rogatory issued under

the IACLR *must* be translated into the language of the receiving nation [IACLR Art 3(b)].



Strategic Point:

If counsel wishes to be able to use the letters in a California court proceeding, it is advisable to have them translated by a certified translator.

14.18[3][b] Letter Should Use Non-Technical Language and No Idioms. Words should be chosen carefully. A letter rogatory should be written in simple and non-technical language and avoid using U.S. idioms that will not translate well.

14.18[3][c] Letter Should Request Production, Not "Discovery." Because most civil law nations will not honor requests for U.S.-style pre-trial discovery, letters rogatory should avoid using the term "discovery" to describe what is being requested. Rather, the letter should request production of computer-based evidentiary materials, or some similar phrase indicating that the request is in compliance with the cultural and judicial norms of the receiving country.



Cross Reference:

Restrictions on common-law style discovery in civil law countries, see 14.06[5].

14.18[4] Requests for ESI or Documentary Evidence Should Be As Specific As Possible. As with letters of request under the Hague Convention, letters rogatory are at their weakest when asking for documents that counsel are not sure the receiving person actually has. Conversely, they are at their strongest when listing specific documents, or categories of documents, which a person (or foreign judicial authority) might reasonably understand that the target person has or is very likely to have.



Warning:

Counsel should not ask for "any and all" documents. A specific list of individual documents should be provided if available.

14.18[5] Counsel Should Request Specific Procedures If Needed. If particular procedures are required for the evidence to be used in California, they should be requested. In the case ESI, particular procedures are needed so that the evidence will be usable in a California court. For example, it is advisable to request a forensically sound collection method by a specialized technician having certain types of certifications or qualifications (EnCe, CCE, CISSP, etc.). The technician should be instructed to provide chain-of-custody type documentation so that the evidence can be entered into evidence [see *Lorraine v. Markel (D Md 2007) 241 FRD 534*]. Counsel should consider locating local technicians or companies that can provide the services, and offering them for use at the parties' expense. If the particular matter has other requirements as to format or otherwise, they should be specified in the letter.



Warning:

If the requirements are too onerous, the local authority can ignore them, or even ignore the letter rogatory completely. The requirements should be simple and easy to understand and comply with. Counsel may need to make do with less than the usual items obtained by U.S.-based technicians. Such a procedure should be discussed with opposing counsel and the court prior to spending time and money on such an ESI production. It is best to have a stipulation that the ESI obtained under the letter rogatory will be deemed admissible.

14.18[6] Counsel Should Prepare a Motion and Order for California Court to Issue Letters Rogatory. Counsel should also prepare a motion and order requesting the California court to issue the letters rogatory. The motion, proposed order, letters, and supporting documentation should be filed in the California court.

14.18[7] Appropriate Documents Should Accompany Letters. For requests under the IACLR [*see* 14.17[3]], the following specific documents must accompany the letters rogatory [*see* Second Inter-American Specialized Conference on Private International Law: Additional Protocol to the Inter-American Convention on Letters Rogatory, May 8, 1979, 18 ILM 1238]:

- A copy of the complaint or pleading that initiated the action in which the letter rogatory was issued, as well as a translation into the language of the state of destination.
- An untranslated copy of any documents attached to the complaint or pleading.
- An untranslated copy of any rulings ordering issuance of the letter rogatory (such as a California court order).
- A form, in the officially specified format, containing essential information for the person to be served or the authority to receive the documents.

➡ **Cross Reference:**

Form, *see* 14.35.

- A certificate, in the officially specified form, on which the Central Authority of the country of destination will attest to execution or nonexecution of the letter rogatory.

➡ **Cross Reference:**

Form, *see* 14.36.

- Under the IACLR, copies will be regarded as authenticated for the purposes of the Convention if they bear the seal of the judicial or administrative authority that issued the letter rogatory [*see* Second Inter-American Specialized Conference on Private International Law: Additional Protocol to the Inter-American Convention on Letters Rogatory, May 8, 1979, 18 ILM 1238].

For ordinary letters rogatory, counsel should consult the website of the foreign nation to determine what documents must accompany the letters. If no specific requirements apply, counsel should consider attaching the documents listed above.



124 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
IV. CONDUCTING FOREIGN E-DISCOVERY USING LETTERS ROGATORY

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.19

AUTHOR: Diane E. Barry, Esq.

14.19 Court Will Forward Letters Rogatory to Foreign Nation.

14.19[1] Letters Rogatory Are Forwarded by Court. The court will forward the letters rogatory to the foreign nation. The letters rogatory must be sent from the California court to the appropriate authority of the receiving nation. Counsel cannot mail them. However, it is frequently the practice for counsel to prepare the mailing materials for the court clerk, which may help expedite processing and avoid transmission errors. Counsel should contact the clerk of the California court to determine the clerk's usual practice and preferences.

Consider:

Any response or correspondence from the other country's courts will be sent to the California court or court clerk, not to counsel.

For letters rogatory submitted under the IACLR, counsel must send two copies to the foreign receiving authority. One is retained by the local authority (often the receiving authority), and one will be served on the actual ESI custodian [see Second Inter-American Specialized Conference on Private International Law: Additional Protocol to the Inter-American Convention on Letters Rogatory, May 8, 1979, *18 ILM 1238*].

14.19[2] Letters Rogatory Issued Through IACLR May Be Presented Through U.S. State Department or Directly to Executing Nation. Letters rogatory issued under the IACLR may be sent through the U.S. State Department, or presented directly to the appointed central authority of the nation with jurisdiction over the person, ESI, or documents [IACLR Art. 4; *28 USC § 1781(a)* (U.S. State Department authorized to receive and forward letters rogatory), (b) (U.S. courts can present letters rogatory directly to foreign nation or court)].

For ordinary letters rogatory, counsel may contact the State Department to see if they are willing to take the letters, or can help counsel decide where to send them. The degree of assistance available may depend on the current relationship with the nation in question.

Strategic Point:



Although it may seem like adding a step, there are advantages to presenting documents through the State Department. Documents presented under the IACLR must be legalized--presented with the court seal [IACLR, Art. 5(a); *see* 14.18[7]]. However, if they are presented through the State Department, the receiving nation will assume that they are properly legalized [IACLR, Art. 6].

14.19[3] Law and Procedures of Executing Nation Will Be Applied. The letters rogatory will be executed in accordance with the law and usual procedures of the receiving nation [IACLR, Art. 10].

14.19[4] Letters Rogatory Will Not Be Executed If Contrary to Public Policy. Signatory nations are authorized to refuse to execute letters rogatory offered under the Convention that are contrary to its public policy [IATLR, Art. 17]. Most civil law states consider that broad-based pre-trial discovery is contrary to their public policy [*see* 14.11[4]].



Cross Reference:

Limiting scope of discovery in civil law states, *see* 14.12[3][b], 14.18[3][c],[4]; *see also* 14.06[5], 14.11[1].

14.19[5] Production of ESI Under Letters Rogatory. Once a letter rogatory has been issued to the appropriate foreign receiving authority, the process of receiving a response and overcoming any objections is much the same as that for a Hague Convention letter of request [*see* 14.13].

The important difference between Hague Convention letters of request and letters rogatory is *enforcement*: The Hague Convention ensures that local authorities will use whatever methods they would use to compel a response to a similar local request. Government authorities receiving and processing letters rogatory make no such promise. In fact, the Inter-American Convention on Letters Rogatory states specifically that compulsion will not be used regarding a letter rogatory [14 ILM 339, Art. 3]. This means that if the recipient refuses to comply with the letter rogatory, the court will not sanction them or otherwise coerce compliance.



125 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions

V. DEALING WITH FOREIGN BARRIERS TO PRE-TRIAL DISCOVERY

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.20

AUTHOR: Diane E. Barry, Esq.

14.20 CHECKLIST: Dealing With Foreign Barriers to Pre-Trial Discovery.

☐ Is desired ESI physically located in nation that belongs to European Union?

Authority:

European Union Directive on Privacy 95 46 EC

Discussion:

See 14.23

☐ Was desired ESI originally controlled by a corporation residing in an EU member nation, and then moved for processing or storage to a place outside the EU?

Authority:

European Union Directive on Privacy 95 46 EC

Discussion:

See 14.23

☐ Does proponent of discovery seek production of information that can identify individuals?

Authority:

European Union Directive on Privacy 95 46 EC

Discussion:

See 14.23[4]

☐ Is desired ESI, document, or witness physically located in a civil law nation?

Authority:

CCP §§ 2026.010, 2027.010

☐ Has nation where ESI is physically located passed laws that specifically block compliance with U.S. legal production obligations?

Authority:

See, e.g., Ontario Business Records Protection Act. R.S.O. 1990, c. B.19, s. 1; French Law No. 80-538, Art. 1

Discussion:

See 14.24

☐ If nation where ESI is physically located has blocking statutes, does counsel have access to local counsel or other local resources in that nation who can negotiate with local ministries regarding desired productions?

Authority:

See, e.g., Ontario Business Records Protection Act. R.S.O. 1990, c. B.19, s. 1; French Law No. 80-538, Art. 1

Discussion:

See 14.16[2]



126 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
V. DEALING WITH FOREIGN BARRIERS TO PRE-TRIAL DISCOVERY

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.21

AUTHOR: Diane E. Barry, Esq.

14.21 Objective and Strategy.

Counsel seeking production of ESI located in another country frequently encounter legal and cultural barriers that exist in foreign nations to block compliance with pre-trial discovery in U.S. litigation matters, including e-discovery. Even if counsel asks for the information correctly, and the producing party acknowledges a duty imposed by California law to produce the e-discovery items, the party seeking discovery still may not be able to obtain production. There are often legal barriers in the foreign nation where the ESI resides that block or impede the producing party's ability to move data from that nation to California. Two major categories of laws in this area are:

- The European Data Privacy Directive [*see 14.23*].
- Blocking statutes in civil law nations [*see 14.24*].

This chapter does not provide a comprehensive discussion of the overall legal framework set out in these statutes, which can have considerable applications outside of ESI production for California litigation. This chapter discusses only aspects that impact California e-discovery participants.



Strategic Point--Keep a Low Profile in Foreign Country:

The first basic strategy in these areas is to *fly low on the legal radar screen*. Be as locally invisible in the foreign nation as possible. If a matter has high visibility (such as being reported in the newspapers or broadcast media), the local nation is more likely to intervene to prevent or hinder productions or to make judgment calls that bar discovery. Visibility usually brings high scrutiny as such a case becomes a public example.

Example:

In a matter that had recently settled as of the date this chapter was written, the United States Government demanded that a Swiss financial institution produce names associated with Swiss bank accounts. The Swiss government absolutely forbade the institution from complying, and threatened to seize the information to prevent the institution from breaching the Swiss banking privacy laws [*see U.S. v. UBS AG (SD FI 2009) No. 09-20423, 2009 US Dist. LEXIS 66739 (court's order denying UBS motion to*

compel the government to disclose which accounts it has identified through other means; can be used as a starting point for tracking this litigation)].



Strategic Point--Be Flexible:

The second strategy is to be flexible. Keep in mind that discovery concerning foreign nationals will always be a diplomatic dance between their national interests and those of our country and state. It will not be all or nothing. It is unlikely to be all our way or all theirs. This is an area that rewards comity among counsel as well as comity among nations. What can be worked out with opposing counsel? Ultimately, counsel should take what can be obtained without argument, and then fight about the rest.



Strategic Point--Consider Informal Channels First:

Finally, counsel should find out what can be obtained informally without breaching foreign legal requirements. With an open mind and creative negotiating, counsel can often get access to some of the things that he or she would like to see, when formal discovery would attract too much notice. It may not be the channel counsel is used to, but it can ease international tensions. As with all informal negotiations, the opposing counsel's willingness to participate matters. If opposing counsel is not as amenable to these discussions as counsel would like, counsel can bring them in front of a California discovery referee or judge who can encourage them to take a better attitude. As a local participant in a California state court matter, local counsel has an edge. The foreign participant can easily end up as the subject of a California court discovery order that demands production, while simultaneously dealing with an irate foreign ministry at home that demands non-production. Both authorities can threaten large fines or even jail time. The opposing party does not want to be in this position, and the proponent of discovery does not want to be without the discovery needed to prove the case. Both parties should have an incentive to negotiate.



127 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
V. DEALING WITH FOREIGN BARRIERS TO PRE-TRIAL DISCOVERY

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.22

AUTHOR: Diane E. Barry, Esq.

14.22 Different Types of Foreign Laws Can Block Flow of E-Discovery Materials to United States.

14.22[1] Foreign Laws Governing Citizens' Rights and Privileges Can Conflict With California Discovery Statutes. It is common for foreign nations to have their own rights and privileges, which they view as more important than a California court's need for litigation materials. Foreign laws often bar or hinder the transfer of ESI outside their borders when the transfer would infringe on important domestic rights and privileges.

Examples:

The European Union Data Privacy Directive and the Swiss banking privacy laws are prime examples of this category of legal barrier.

14.22[2] Foreign "Blocking Statutes" Can Expressly Target Discovery of Citizens. As a second and distinct category, many nations view U.S. discovery practices as harassment of their citizens, as well as an infringement on domestic government authority. Many nations have passed laws that protect their citizens from the burden of responding to this kind of intrusion. These types of laws are known as "blocking statutes."



Cross Reference:

Blocking statutes, see 14.24.

14.22[3] Judicial Respect Accorded to Foreign Laws Varies According to Nature and Purpose of Statute. Laws that protect essential rights and freedoms of foreign nationals, such as the EU Data Privacy Directive, receive a significant amount of judicial respect in the United States. It is likely that counsel will not be able to simply ignore them. Discovery requests may need to be curtailed, and more limited compliance negotiated with care and flexibility.

Example--Foreign Banking Law Protects Substantial Interest:

In *Minpeco, S.A. v. Conticommodity Servs., Inc.* (SDNY 1987) 116 FRD 517, 527-528, the court held that the Swiss Bank Secrecy Law protected a substantial interest in bank client account information.

Blocking statutes, in contrast, have no real purpose other than to thwart litigation demands, and need not be afforded the same respect as laws that protect significant foreign rights and interests [Restatement (Third) of The Foreign Relations

Law § 442 (1987) ("adjudication should take place on the basis of the best information available [and] ... statutes that frustrate this goal need not be given the same deference by courts of the United States as differences in substantive rules of law").



128 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
V. DEALING WITH FOREIGN BARRIERS TO PRE-TRIAL DISCOVERY

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.23

AUTHOR: Diane E. Barry, Esq.

14.23 The EU Data Privacy Directive and Member Enforcement Laws.

14.23[1] Right to Privacy Is Recognized by European Union. The right to privacy is acknowledged in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, as well as the laws of the individual member nations, and is implemented by the EU Data Privacy Directive. The official name of this directive is Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data. It is referred to in this chapter as the EU Data Privacy Directive. The legal citation is EU Directive 95 46 EC.

The purpose of the EU Data Privacy Directive is to remove obstacles to the flow of personal data, often required for use commerce, while still protecting the privacy of the individuals whose data is involved. The directive accomplishes this by creating a standard set of protections for personal data that must be offered in each EU member nation. Thus, wherever it goes in the EU, personal information is protected [EU Directive 95 46 EC, 1995 OJ L 281, Preamble, sections (8), (9)]. The directive is intended to implement the conclusions of the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data [EU Directive 95 46 EC, 1995 OJ L 281, Preamble, section (11)].



Cross Reference:

Full text of EU Data Privacy Directive on lexis.com, see 1995 OJ L 281.

14.23[2] EU Data Privacy Directive Binds All EU Member States. The European Union's legislative body issues directives, which are then to be implemented through domestic legislation by each EU member nation. Domestic legislation implementing a directive is usually referred to as a "member enforcement law." EU member states are required to protect the personal data of EU citizens in accordance with the provisions of the EU Data Privacy Directive [EU Directive 95 46 EC, 1995 OJ L 281, Art. 1].



Warning:

The EU directives are binding upon the member nations whether they create member enforcement laws

or not. Member enforcement laws merely set out the local methods the member nation will use to comply with the EU directive.

As of mid-2009, the member states of the European Union are: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom. For a current list, see the official EU website: http://europa.eu/abc/european_countries/index_en.htm.

14.23[3] Directive Applies to Any Entity Subject to EU Community Law. The Directive applies to any entity subject to EU community law, whether the entity is physically located inside the EU or not [EU Directive 95 46 EC, 1995 OJ L 281, Art. 4].

Exceptions:

The use of personal data by natural persons for purely personal or household purposes (such as correspondence) is excluded [EU Directive 95 46 EC, 1995 OJ L 281, Art. 3]. Various government uses are also excluded [EU Directive 95 46 EC, 1995 OJ L 281, Art. 3 (criminal and state security matters)].

14.23[4] Directive Presents Significant Obstacle for Litigation in U.S. Courts. The EU Data Protection Directive presents a tremendous challenge in U.S. litigation matters when the production includes information that can uniquely identify individual persons:

- First, the EU standards for what is considered private personal information are very different from anything applied by even stringent U.S. venues such as California. The considerations are very foreign to our legal ways of thinking, and most of the EU concerns would not present a barrier to U.S. legal productions.
- In addition, this directive is a legal requirement on the entity in possession of the data. Compliance is not negotiable and cannot be eased by something as simple as a confidentiality agreement or stipulation. If the information is personal data under EU definitions, the hosting entity's ability to move or process the information is severely limited. Obtaining discovery of EU personal data requires planning, cultural sensitivity, cooperation, and perseverance.

14.23[5] Directive Regulates Activities of "Controllers" of Regulated Personal Data. The EU Data Privacy Directive seeks to regulate the activities of "controllers," the persons or entities that decide what the data is to be used for, and who control the "processing" of the data [EU Directive 95 46 EC, 1995 OJ L 281, Art. 2(d)]. For the purposes of this practice guide, a party attempting to produce personal data in its custody or control comes within the definition of a "controller" of the information. The EU Privacy Directive Controllers regulates what "processing" they can perform on personal data in their possession or control, and where they can move it.

14.23[6] Directive Regulates Processing or Movement of "Personal Data." The EU Data Privacy Directive applies to [EU Directive 95 46 EC, 1995 OJ L 281, Arts. 1 and 2]:

- "processing"
- or cross border movement
- of "personal data"
- stored in an automated structured filing system that permits easy access to personal data.

- by any entity subject to EU community law.

"Personal data" is any information about any "identified or identifiable natural person" [EU Directive 95 46 EC, 1995 OJ L 281, Art. 2(a)]. A natural person is "identified or identifiable" if that person can be uniquely identified, directly or indirectly, by reference to the stored information. Such persons are referred to in the Directive as "data subjects."

Examples are identification numbers, or combinations of stored factors regarding a natural person's physical, physiological, mental, economic, cultural, or social identity [EU Directive 95 46 EC, 1995 OJ L 281, Art. 2(a)]. The identification factors require that practitioners consider the data set as a whole. What is actually in the data set? Just because the information pertains to natural persons does not mean that it would permit the unique identification of any of the individuals. Conversely, even if individual entries do not identify a unique individual, if the dataset is considered as a whole, it might do so. The more data points there are in the target dataset, and the more particular the data points are, the more likely it is that a unique person can be identified.

Examples--Unique Identification Examples.

- The facts that someone is a Sudanese citizen and is living in France might not be enough to identify a unique individual. However, if the database also holds information on body scars and childhood medical background, the dataset, taken as a whole, probably could identify a unique individual.
- It might not be enough to know that the data pertains to a citizen of the Czech Republic who likes jazz music, but what if it also shows that his or her mother taught at the University of Lancaster?

Strategic Points:



- Production of a complete database or other structured dataset is not required in all cases. Counsel should assess what information is actually needed. If the necessary materials contain an identification number, such as a passport number or a social security number equivalent, or a credit card number or bank account number, then it will still identify a unique individual. But it is possible that the information counsel actually needs would not implicate the Data Privacy Directive. If counsel can make do with a subset, would the subset, looked at as a whole, uniquely identify natural persons? It is worth considering and negotiating with opposing counsel.

- A good way to find out about the information source and what counsel actually need from it is to take the deposition of a person knowledgeable about what it contains. A deposition should not itself implicate the data directive, although counsel may need to comply with Hague Convention or letters rogatory regarding the taking of evidence from witnesses who are located abroad. Counsel should ask for description manuals and a data dictionary (description of the information that ought to be in the specific fields of the database) and question the person most knowledgeable about the data.



Cross Reference:

For further discussion on taking a deposition in a foreign nation, see *Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 7, Taking Oral Depositions Outside of California, 7.10-7.16.*

14.23[7] Directive Regulates Personal Data Collections and Forbids Later Processing for Different Purposes.

Personal data may only be gathered for a specified legitimate purpose [EU Directive 95 46 EC, 1995 OJ L 281, Art. 6]. Once in the possession of a "controller," it cannot be processed again later for some purpose that is incompatible with

the originally specified purpose [EU Directive 95 46 EC, 1995 OJ L 281, Art. 6]. Later processing is permitted only if it meets one of the specific exemptions set out in the directive [EU Directive 95 46 EC, 1995 OJ L 281, Arts. 6-8].

14.23[8] Litigation Production Preparation Steps Are "Processing" Within Meaning of Directive.

"Processing" refers to almost any action that can be performed on ESI, including collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction [EU Directive 95 46 EC, 1995 OJ L 281, Art. 2(b)]. Every step a producing party would need to take in order to prepare an ESI production in California litigation meets the definition of "processing." Typically, the responding party would need to search, identify, retrieve, collect, manipulate, and produce the target ESI in a reasonable litigation format. Privilege review would require "consultation" of the data. Each of those steps is described in the Directive's definition of "processing" [EU Directive 95 46 EC, 1995 OJ L 281, Art. 2(b)].

Therefore, if the target ESI contains personal data, the Directive bars *the entire process of responding to discovery requests*, unless this process can be fitted into one of the permissible exemptions.

14.23[9] Exemptions May Apply to Permit Litigation Processing in Some Situations.

14.23[9][a] Data Subjects Can Consent to Later Processing. A data subject can consent to later processing of personal data for different purposes. The consent must be specific and unambiguous [EU Directive 95 46 EC, 1995 OJ L 281, Art. 6(a)]. Compliance with this section usually would require special notice to each data subject, and subsequent consent [EU Article 29 Data Protection Working Party, EU Working Document 1/2009 on pre-trial discovery for cross border civil litigation, pp. 8-9].

14.23[9][b] Later Processing Permitted to Comply With Legal Obligations. Later processing may be permitted if necessary to comply with a legal obligation to which the controller is subject [EU Directive 95 46 EC, 1995 OJ L 281, Art. 6(c)].

Although this exemption looks promising, the EU's Article 29 Data Protection Working Party has opined that this section would not apply if the legal obligation were only a foreign statute or regulation. However, it further states that this section might apply if the domestic laws of the controller's nation required compliance with foreign orders [EU Article 29 Data Protection Working Party, EU Working Document 1/2009 on pre-trial discovery for cross border civil litigation, p. 9]. The Working Document also states that this obligation could exist even if the nation had filed an exemption from pre-trial discovery under the Hague Convention Article 23, as long as the controller was required to make a pre-trial disclosure [EU Article 29 Data Protection Working Party, EU Working Document 1/2009 on pre-trial discovery for cross border civil litigation, p. 9].

The author has been unable to locate case law that interprets or applies this section.

14.23[9][c] Processing May Be Permitted If Necessary for Controller's Legitimate Interests. Processing for the pursuit of the legitimate interests of the controller is permitted, unless such interests are overridden by the rights set out in Article 1 of the EU Data Privacy Directive [EU Directive 95 46 EC, 1995 OJ L 281, Art. 6(f)]. This section has been construed to authorize limited litigation production. Litigation can be a legitimate interest of the controller [EU Article 29 Data Protection Working Party, EU Working Document 1/2009 on pre-trial discovery for cross border civil litigation, pp. 9-10].

The exemption sets out a balancing test, permitting an examination of the litigation need for the information versus the depth of the infringement and the importance of the right being infringed. This "balance of interest test" should consider the relevance of the personal data to the litigation and the consequences for the data subject of exposure [EU Article 29 Data Protection Working Party, EU Working Document 1/2009 on pre-trial discovery for cross border civil litigation, p. 10].

Consider:

The controller should consider whether there are ways to produce only information that is directly relevant. Perhaps certain pieces of sensitive data can be redacted, or replaced with a pseudonym [EU Article 29 Data Protection Working Party, EU Working Document 1/2009 on pre-trial discovery for cross border civil litigation, p. 11].

14.23[9][d] Processing May Be Permitted If Necessary for Defense of Legal Claims Within EU. The EU Data Privacy Directive specifically authorizes the processing of personal data when the publication is "necessary for the establishment, exercise or defense of legal claims" [EU Directive 95 46 EC, 1995 OJ L 281, Art. 8, § 2(e)]. However, this section applies only to the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life [EU Directive 95 46 EC, 1995 OJ L 281, Art. 8, § 1]. It is generally construed to apply only to EU court or regulatory matters. For example, it is not addressed at all in the Article 29 Working Group's Working Document 1/2009 on pre-trial discovery for cross-border civil litigation.

14.23[10] Directive Also Regulates Cross-Border Movement of Personal Data.

14.23[10][a] Directive Imposes Limitations on Movement of Information. In addition to "processing," the EU Data Privacy Directive regulates where the information can be moved; that is, whether or not it can be moved to California after processing [EU Directive 95 46 EC, 1995 OJ L 281, Arts. 25, 26 (transfer of personal data to third countries)]. If counsel is able to overcome the "processing" hurdles, the restrictions on movement of personal data still must be overcome.

14.23[10][b] Data May Be Transferred If "Adequate Level of Protection" Exists. A controller may transfer personal data freely to a third country (that is, a non-EU member state), if the third country ensures "an adequate level of protection" [EU Directive 95 46 EC, 1995 OJ L 281, Art. 25, subsection 1]. Essentially, to be an approved destination, the third country must provide much the same data protections as are imposed on EU nations by the Directive. As of mid-2009, the EU has formally designated only Argentina, Canada, Guernsey, Isle of Man, and Switzerland as approved third countries for movement of personal data.

14.23[10][c] United States Is Not an Approved Destination for Personal Data, but Individuals Can Apply for Approval Under Safe Harbor in Directive. The United States does not qualify as an approved destination, because U.S. laws do not provide the desired level of protection for personal data. However, *individuals* within the United States can apply for approval as a destination under Safe Harbor provisions authorized by the EU [see 2000/520/EC, Commission Decision of 26 July 2000 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 related frequently asked questions issued by the U.S. Department of Commerce], and implemented in the United States by the U.S. Department of Commerce. Essentially, the company must implement data security protocols equal to those used in the EU and register with the U.S. Department of Commerce.

The criteria required to claim the safe harbor certification are published by the Department of Commerce [see http://www.export.gov/safeharbor/eu/eg_main_018365.asp]. The Department of Commerce also maintains a list of those entities that have certified themselves as compliant with the safe harbor provisions, and are therefore presumably approved destinations for receipt of EU personal data [see <http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list>].

**Strategic Point--Negotiate Production to Safe Harbor Company in United States:**

If counsel can successfully negotiate a data production that meets the Directive's processing exemptions [see 14.23[9][b], [c], [d]], counsel then can request production to a safe harbor company located in the

United States, which can host the ESI for litigation use. This would constitute approved processing and movement to an approved destination [see 2000/520/EC, Commission Decision of 26 July 2000 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 related frequently asked questions issued by the US Department of Commerce].

14.23[11] Data Subjects Have Personal Right to Sue for Infringement. The EU Data Privacy directive gives each data subject a personal right to sue the controller for failure to protect their rights as required by the Directive [EU Directive 95 46 EC, 1995 OJ L 281, Arts 22--24].

Consider:

One of the problems in negotiating productions of personal data is that foreign government or ministry blessing may not be sufficient to shield a controller from adverse effects.



129 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
V. DEALING WITH FOREIGN BARRIERS TO PRE-TRIAL DISCOVERY

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.24

AUTHOR: Diane E. Barry, Esq.

14.24 Blocking Statutes May Pose Barrier to ESI Production.

14.24[1] Blocking Statutes Specifically Address Foreign Litigation. A "blocking statute" is a foreign law enacted "for the express purpose of frustrating the jurisdiction of the United States courts" [*see In re Uranium Antitrust Litigation* (ND Ill 1979) 480 F Supp 1138, 1143] .

Examples:

- The Ontario Business Records Protection Act [RSO 1990, c. B.19, s. 1] generally forbids the movement of business records from Ontario to any place outside of Ontario unless that movement is part of the regular business of the company. Litigation in the United States is not construed as being part of the regular business of a company. The act authorizes the Attorney General to take steps to ensure compliance. If the Attorney General or any other interested person has reason to believe that a regulated business is, or is about to become, the subject to an order, direction, or summons that might require it to breach this provision, the business can be ordered to furnish an undertaking to ensure compliance with the Act.

- French Law No. 80-538 forbids requesting or furnishing "documents or information of an economic, commercial, industrial, financial, or technical nature directed toward establishing evidence in view of legal or administrative proceedings abroad or in relation thereto" [French Law No. 80-538, Art. 1]. Breach is punishable by imprisonment for up to six months, and/or fines.

14.24[2] Blocking Statutes Are Not Always Enforced by Foreign Nation. More than one federal court has noted that blocking statutes are often a paper tiger--threat and no enforcement [*see Adidas Ltd. v. SS Seatrain Bennington* (SDNY 1984) 1984 US Dist. LEXIS 16300 ("[t]he legislative history of the [French blocking] statute gives strong indications that it was never expected or intended to be enforced against French subjects but was intended rather to provide them with tactical weapons and bargaining chips in foreign courts")]. The sole reported case enforcing the French blocking statute that was found at the time this chapter was written fined the counsel in question the lowest fine permissible under the statute [*see Cour de Cassation Chambre Criminelle* [Cass Crim], Paris, Dec 12, 2007, Juris-Data

no. 2007-332254].

Example--Counsel Fined for Requesting Document Regulated by French Law No. 80-538:

In 2007, a French mutual insurance company was a defendant in litigation brought in federal court in Los Angeles. A French lawyer working with a U.S. firm representing the California Insurance Department phoned the French firm attempting to obtain some information informally. He was charged under French Law No. 80-538, and fined 10,000 euros. The fine was upheld on appeal [Cour de Cassation Chambre Criminelle [Cass. Crim.], Paris, Dec 12, 2007, Juris-Data no. 2007-332254].

14.24[3] United States Courts Accord Lesser Judicial Respect to Blocking Statutes. Even if blocking statutes are enforced, they are not entitled to the same kind of judicial respect as those laws that protect substantial foreign rights and privileges [see, e.g., *Minpeco, S.A. v. Conticommodity Servs., Inc.* (SDNY 1987) 116 FRD 517, 527-528 (Swiss Bank Secrecy Law protected the substantial interest in the protection of bank client account information); Restatement (Third) of the Foreign Relations Law § 442 (1987) ("adjudication should take place on the basis of the best information available [and] ... statutes that frustrate this goal need not be given the same deference by courts of the United States as differences in substantive rules of law")].



130 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
VI. EVALUATING PRACTICAL AND TECHNICAL CONSIDERATIONS IN FOREIGN E-DISCOVERY

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.25

AUTHOR: Diane E. Barry, Esq.

14.25 CHECKLIST: Evaluating Practical and Technical Considerations in Foreign E-Discovery

- ☐ Review State Department website for information on current judicial and legal resources available for country where foreign ESI is located.

Discussion:

See 14.16

- ☐ Consider associating counsel located in target foreign nation.

Discussion:

See 14.16[1]

- ☐ Does counsel have a relationship with a collection vendor who can handle collections in country where ESI is located?

- ☐ If so, is vendor prepared to provide a local witness who can answer court questions regarding collection?

Discussion:

See 14.28[1]

- ☐ When production is obtained, what language or languages will be shown?

Discussion:

See 14.29

☐ Will counsel's current computerized review tools do the following:

☐ Load and show characters from that language?

☐ Search in that foreign language?

☐ Does counsel need to arrange for a different tool to handle ESI for this matter?

Discussion:

See 14.29[4]-14.29[6]

☐ Will ESI review be conducted in original language, or will it need to be translated?

Discussion:

See 14.29[1]



131 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
VI. EVALUATING PRACTICAL AND TECHNICAL CONSIDERATIONS IN FOREIGN E-DISCOVERY

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.26

AUTHOR: Diane E. Barry, Esq.

14.26 Objective and Strategy.

The practical aspects of dealing with foreign ESI need to be considered by anyone involved with it--plaintiffs, defendants, experts, and even third parties producing evidence to the matter.

Example:

If counsel needs to produce e-mail and databases from the Ukraine (Cyrillic alphabet), must anything special be done to collect it? What if it was created using a local Ukrainian e-mail program, and not Microsoft Exchange or Lotus Notes? Once it has been collected, how will it be reviewed? What if the Ukrainians were corresponding with sales departments in Nigeria and South Korea?



Strategic Point:

The best time to consider these issues is early in the litigation. From identification through production, dealing with foreign language materials requires planning and use of different tools and methods than can be used for entirely English programs and materials. Early planning saves money, as work will not need to be redone and data will not need to be moved from one kind of tool to another in order to perform all of the tasks required.



132 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
VI. EVALUATING PRACTICAL AND TECHNICAL CONSIDERATIONS IN FOREIGN E-DISCOVERY

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.27

AUTHOR: Diane E. Barry, Esq.

14.27 Practical Considerations Must Be Considered in Any Cost-Benefit Analysis.

Obtaining discovery of ESI from foreign jurisdictions is more time consuming and difficult than obtaining ESI located in California or even elsewhere in the United States. Technical support costs also can be significantly higher for foreign ESI than domestic ESI. For example, foreign language ESI must be collected properly in a foreign nation, and tools to deal with foreign language ESI cost more



Cross Reference:

Authentication of evidence at trial, see *Ch. 15, Admissibility of Electronic Evidence, 15.12-15.17*.

Before conducting e-discovery in a foreign jurisdiction, counsel should ask whether the matter itself, and the desired ESI evidence in particular, are worth the time and expense of going after it. If the same or substantially similar information can be obtained anywhere within the boundaries of the United States, the answer to this question should be an emphatic "no."



133 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
VI. EVALUATING PRACTICAL AND TECHNICAL CONSIDERATIONS IN FOREIGN E-DISCOVERY

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.28

AUTHOR: Diane E. Barry, Esq.

14.28 Counsel Must Decide How to Address Technical Collection Issues in Foreign E-Discovery.

14.28[1] Counsel Must Decide Whether to Hire Foreign or U.S. Vendors for ESI Collection. If counsel is representing the ESI data source, counsel will need to work with the client to arrange for data collection in accordance with U.S. standards.

A local foreign vendor has the advantages of language and often parochial preference--for example, a Japanese discovery target might prefer to have its ESI collected by a Japanese e-discovery vendor. A local vendor will be aware of local cultural sensitivities and use locally-designed software or hardware. A local vendor also can be less expensive--no travel expenses and lower local prices.

Conversely, there are distinct problems associated with using a foreign vendor. First is the question of whether or not its personnel are knowledgeable about U.S. evidence collection standards. If not, it may be difficult to get the evidence authenticated once collected.

Second, if there are questions about the collection, and the court wants to talk to someone involved in the actual collection, or the opponent wants to take a PMK deposition, it may be difficult to figure out whom to put on the stand. There may be issues with the person's English skills and comfort level with a California court proceeding. If the person does not want to appear personally, it may be difficult to compel appearance. Even if he or she is willing to come, there is the expense of preparing a foreign witness--travel and translation expense can be significant.

Strategic Points:



- For the reasons discussed above, it is usually better to hire a U.S. collection company with offices abroad in or near the place where the data is located. Counsel can get a U.S.-based project manager, often one who can testify if necessary. If counsel needs to subpoena the vendor for some reason, the U.S. office can be subpoenaed.

- If counsel decides to work with a local foreign vendor for collections, consider sending a U.S. project manager to oversee the work. This project manager can be from counsel's own firm (if the person's credentials are appropriate) or can be hired from an outside collections vendor. This project manager must be bilingual, or counsel will need to arrange for a translator.

- A U.S.-based project manager can provide most, if not all, the testimony that might be required to address discovery process questions, and will be locally available and have good English skills. Such a person also is better able to provide assurance that the end work product conforms to U.S. evidentiary standards.

14.28[2] Collection Must Be Unicode Compliant. In order to transfer data reliably from foreign systems into a document review and analysis program, Unicode compliant collection is a necessity.

Unicode is a data encoding standard that maps the characters and symbols used in various writing systems to a common definition, so that a given character will always have the same binary representation. Prior to Unicode, different encoding standards, e.g. Latin 1 or Windows Code Page 1251, each used the same binary codes to represent different characters. What this means, in practical terms, is that without Unicode, it is not possible to reliably transfer the same foreign language characters from one system to another. The code for a character will differ from system to system.

Consider:

Microsoft Outlook systems that are newer than Outlook 97 store data by default as Unicode.



134 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
VI. EVALUATING PRACTICAL AND TECHNICAL CONSIDERATIONS IN FOREIGN E-DISCOVERY

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.29

AUTHOR: Diane E. Barry, Esq.

14.29 Counsel Must Decide How to Address Issue of Foreign Language Document Review.

14.29[1] Review Must Be Conducted in English, Foreign Language, or a Combination of the Two. Counsel must decide how to read the documents that need to be read. The basic choices are:

- Hire foreign language speaking attorneys to conduct the review.
- Have the documents translated into English.
- Some combination of the above.

In addition, the computer tools that will be needed must be able to support the review staff selected for the task.

Example:

Counsel will need different tools to conduct a review in Arabic than if the documents are translated into English first.

14.29[2] Bilingual Staffing May Make Review Much Easier. One solution to the language issue is for counsel's firm to have staff attorneys who can read and write in the target language. If the firm is located in a multicultural area, hiring bilingual review staff is also an option. This option means that most of the ESI that is collected will not need to be translated. Only those items that will actually be presented to a witness or in court will need to be translated. Original language review also provides the advantage of cultural sensitivity: many nuances of language do not translate well, and can be picked up by original language review.



Warning:

Make certain that any bilingual review staff have sufficient reading and writing skills in the language in question, as opposed to just spoken language skills, to be able to analyze written materials for legal review purposes.

14.29[3] Translation Is Required If Documents Are Reviewed in English. If review will be conducted by English-speaking attorneys, the documents must be translated. Documents that will be presented in court must be translated by a court-certified translator. This is an expensive endeavor and can cost thousands of dollars per banker's box of materials.

A better strategy is to employ machine translation for the bulk of the documents, conduct a review, and then have selected documents translated by the more expensive method. Machine translation costs a few hundred dollars a box, rather than tens of thousands. If a document is "hot" or will be presented to a witness or to the court, the additional cost of a court-certified translator is then justified.

14.29[4] Search Tools Must Be Selected Carefully. Counsel must decide what tools will be used to review the ESI once it has been successfully obtained. The following questions should be considered:

- Is counsel's usual review tool capable of taking foreign language ESI data?
- Can it load Unicode ESI data?
- Will it show Cyrillic, Arabic, kanji, or other characters?
- Can it search ESI using those character sets?



Strategic Points:

If counsel's usual in-house tool cannot handle the foreign language ESI, consider using an online tool hosted by a vendor. If this is counsel's only case that requires this capacity, it is not necessary to switch in-house tools. Counsel simply needs additional assets for this one matter. An online tool is "pay as you go"--counsel can pay for it for this one case only, and the law firm does not need to acquire capacity it doesn't need for other matters. Furthermore, in such a case the costs are case specific and can be passed along to the client.

14.29[5] Cross-Lingual Search Tools Are Available. Counsel should consider whether it is worth investing in a cross-lingual search tool. A cross-lingual tool translates searches into each language used in the ESI. For example, counsel can search using English terms, and the program will return all appropriate documents, whether in English or Cyrillic, Arabic, kanji, or whatever language is designated. Searches can also be conducted in the foreign language by entering search terms in that language. A good cross-lingual tool works even in multilingual data sets; for example, one containing e-mail in Korean, Japanese, Cantonese, and English.



Strategic Points:

- A cross-lingual tool is useful for ESI that either has not yet been translated, or will not be translated. It permits English-speaking attorneys to see if certain concepts or key terms are present in the data.
- A cross-lingual tool is useful for mixed language review teams. It also enables both English speakers and foreign language speakers to work with the same data. They can search in English or a foreign language.

14.29[6] Conceptual Search Tools Allow Concept-Based Searching. Conceptual searching is much more precise

than simple term searching. A conceptual search tool will return records that are related to a concept, as opposed to those where a specific term or set of terms appear. Conceptual tools allow the user to enter terms or document text and then search for records in the ESI dataset that are strongly correlated to the target concept. This is useful when the concept is called different things in different cultures or legal systems. It can also be useful when different departments of a company refer to the same projects in different ways.

Example:

Consider how many different interpretations of the word "bill" there are. Is counsel interested in invoices, or William, or California legislature bill AB5? A conceptual search tool can focus on the desired significance of a term and weed out the numerous false positives when the word is right but not the concept. This provides costs savings by reducing expensive review time. It also pulls in documents in which the terms did not appear, but which are indeed related to the concept. Counsel gets less "noise" and more relevant material.



135 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
VII. FORMS*1-14 MB Practice Guide: CA E-Discovery and Evidence 14.30***AUTHOR:** Diane E. Barry, Esq.**14.30 Notice of Motion and Motion for Issuance of Letters Rogatory or Letter of Request.**

Notice of Motion and Motion for Issuance of Letters Rogatory or Letter of Request.

Tom Doe

California Bar Number 987654

100 North Main St., Suite 200

Farallon City, California 90000

Phone: 555-555-5555

Attorney for Plaintiff, John Smith

SUPERIOR COURT OF CALIFORNIA,

COUNTY OF FARALLON

	)	
	)	No. _____
	)	NOTICE OF MOTION AND MOTION FOR ISSU-
	)	ANCE OF _____ [LETTERS ROG-
John Smith, Plaintiff, vs. Mary Jones Enterprises,	)	ATORY <i>or</i> LETTERS OF REQUEST] TO OBTAIN
Inc., Defendant.	)	PRODUCTION OF ELECTRONICALLY STORED
	)	INFORMATION LOCATED OUTSIDE OF THE
	)	UNITED STATES
	)	DECLARATION OF _____ (name)]
	)	Date: _____
	)	Time: _____
		Location: _____
		Judge: _____
		Date Action Filed: _____
		Trial Date: _____

To DEFENDANT MARY JONES and to his/her attorney of record:

NOTICE IS HEREBY GIVEN that on _____, at _____ [time], or as soon thereafter as the matter may be heard, in _____ [Department or Division] of this court, located at _____ [street address], _____ [city], [identify moving party, e.g., Plaintiff John Smith] will, and hereby does, move the court for issuance, out of and under its seal, of _____ [Letters Rogatory or a Letter of Request] requesting the appropriate judicial authority in _____ [name of foreign nation] to obtain production of specified electronically stored information.

This motion will be made on the grounds that:

1. The electronically stored information described in the _____ [letters rogatory or letter of request] is located outside the boundaries of the United States; and
2. Within the boundaries of _____ [country], a nation _____ [for a letter of request: which is a signatory to the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters or, for letters rogatory: where issuance of letters rogatory are necessary to obtain production of the ESI required]; and
3. That _____ [identify moving party, e.g., Plaintiff John Smith] is entitled to obtain production of this information, and
4. That it is _____ [necessary and/or convenient] that the _____ [Letters Rogatory or Letter of Request] issue.

The motion will be based on this notice of motion, on the declaration of _____ [name] filed in support thereof, and the memorandum of points and authorities served and filed herewith, on the records and file herein, and on such evidence as may be presented at the hearing of the motion.

Dated: _____

_____ [firm name]

By: _____ [signature]

_____ [typed name]

Attorney for _____

SUPPORTING DECLARATION OF _____ [name]

I, _____ [name], declare:

1. I am _____ [identify declarant, e.g., an attorney at law duly admitted to practice before all the courts of the State of California and the attorney of record herein for Plaintiff John Smith in the action described above]. I am over the age of 18, and if called as a witness, I could and would competently testify to facts set out in this declaration.
2. _____ [Name of moving party, e.g., Plaintiff John Smith] is seeking an order of this court for issuance of _____ [Letters Rogatory or a Letter of Request] requesting the appropriate judicial authority in _____ [name of foreign nation] to take the necessary steps to obtain production of the electronically stored information ("ESI") described in the _____ [Letters Rogatory or Letter of Request] filed with this motion.

3. The desired ESI is _____ [located/owned/controlled by] _____ [name of entity or person] located at _____ [foreign address].
 _____ [Name of foreign nation, e.g., Brazil] is _____ [for letters of request: a signatory to the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters or, for letters rogatory: a nation for which letters rogatory are necessary to request judicial assistance to obtain production of ESI within its territorial boundaries].

4. [If there are any agreements with the ESI custodian regarding acceptance of a request made via letters rogatory or letter of request, provide particulars of those agreements here. Attach any documentation as exhibits to this declaration.]

5. [If the ESI custodian is a party to the litigation: This motion and issuance of _____ (the letter of request or letters rogatory) does not waive the requesting party's right to proceed under the California Code of Civil Procedure at a later date].

6. It is _____ [necessary and/or convenient] that this court issue _____ [Letters Rogatory or a Letter of Request], in that _____ [specify, in accordance with requirements of foreign jurisdiction]. I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Dated: _____
 _____ [firm name]
 _____ [typed name]

MEMORANDUM OF POINTS AND AUTHORITIES

[Set out memorandum here]

NOTES:

Authority:

Hague Convention for Evidence, Art. 1; CCP §§ 2026.010, 2027.010; 14 ILM 339; 14 ILM 1238; 23 UST 2555

Discussion:

See 14.12, 14.18

Related Form for Order:

See 14.31



136 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
VII. FORMS*1-14 MB Practice Guide: CA E-Discovery and Evidence 14.31***AUTHOR:** Diane E. Barry, Esq.**14.31 Proposed Order for Commission, Letters Rogatory, or Letter of Request for Deposition in Foreign Nation.**Proposed Order for Commission, Letters Rogatory, or Letter of Request for Deposition in Foreign Nation.
SUPERIOR COURT OF CALIFORNIA,
COUNTY OF FARALLON

	)	
	)	No. _____
	)	ORDER FOR ISSUANCE OF
	)	_____ [LETTERS ROGATORY or
John Smith, Plaintiff, vs. Mary Jones Enterprises,	)	LETTER OF REQUEST TO OBTAIN PRODUC-
Inc., Defendant.	)	TION OF ELECTRONICALLY STORED INFORM-
	)	ATION LOCATED OUTSIDE THE UNITED
	)	STATES]
	)	Date: _____
	)	Time: _____
		Location: _____
		Judge: _____
		Date Action Filed: _____
		Trial Date: _____

Application having been made by PLAINTIFF JOHN SMITH for an order that _____ [letters rogatory or a letter of request] issue to request foreign judicial assistance in obtaining production of specified electronically stored information located in _____ [name of nation], proof having been made to the satisfaction of the court, and good cause appearing therefor,

IT IS ORDERED that _____ [Letters Rogatory or Letters of Request] issue out of and under the seal of this court and directed to the judicial authorities of _____ [name of nation], requesting assistance in obtaining production of the specified electronically stored information.

Dated: _____

_____ [*Typed name of Judge*]

Judge of the Superior Court

NOTES:

Authority:

14 ILM 339 Art. 4

Discussion:

See 14.12, 14.18.

Related Form for Motion and Notice of Motion:

See 14.30



137 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
VII. FORMS

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.32

AUTHOR: Diane E. Barry, Esq.

14.32 Letter of Request for Service Abroad, With Certification of Service--Hague Convention Form (U.S. Marshals Service Form USM94).

Letter of Request for Service Abroad, With Certification of Service--Hague Convention Form (U.S. Marshals Service Form USM94).

[Click here to view image.](#)

NOTES:

Source of Form:

U.S. Department of Justice, U.S. Marshals Service, Form USM-94,
<http://www.usmarshals.gov/forms/usm94.pdf>

Authority:

Hague Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or
Commercial Matters

Use of Form:

Use of this official form is not required, but is recommended to assure that the form complies with
Hague Convention requirements

Discussion:

See 14.10-14.13



138 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
VII. FORMS*1-14 MB Practice Guide: CA E-Discovery and Evidence 14.33***AUTHOR:** Diane E. Barry, Esq.**14.33 Model for Letters of Request Recommended for Use in Applying the Hague Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters.**

Model for Letters of Request Recommended for Use in Applying the Hague Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters.

Request for International Judicial Assistance pursuant to the Hague Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters

*N.B. Under the first paragraph of article 4, the Letter of Request shall be in the language of the authority requested to execute it or be accompanied by a translation into that language. However, the provisions of the second and third paragraphs may permit use of English, French or another language.**In order to avoid confusion, please spell out the name of the month in each date.**Please fill out an original and one copy of this form (use additional space if required).*

1. Sender _____ (identity and address)
2. Central Authority of the Requested State _____ (identity and address)
3. Person to whom the
executed request is to be returned _____ (identity and address)
4. Spec-
 tifica-
 tion
 of the
 date
 by

which
the re-
quest-
ing
au-
thor-
ity re-
quires
re-
ceipt
of the
re-
spons
e to
the
Letter
of Re-
quest

Date _____
Reason for urgency* _____
* Omit if not applicable.

IN
CON-
FOR
MITY
WIT
H
ART-
ICLE
3 OF
THE
CON-
VEN-
TION
, THE
UN-
DER-
SIGN
ED
AP-
PLIC
ANT
HAS
THE
HON-
OUR
TO
SUB-
MIT

THE
FOL-
LOW
ING
RE-
QUE
ST:

5. *a* Requesting judicial authority (article 3,a) _____ (*identity and ad-
dress*)
- b* To the competent authority of (article 3,a) _____ (*the requested
State*)
- c* Name of the case and any identifying _____
 number
6. Name
 s and
 ad-
 dresse
 s of
 the
 partie
 s and
 their
 rep-
 re-
 sent-
 atives
 (inclu
 ding
 rep-
 re-
 sent-
 atives
 in the
 re-
 ques-
 ted
 State*)
)
 (article
 3,b)
- a* Plaintiff _____
 Representatives _____
- b* Defendant _____
 Representatives _____
- c* Other parties _____
 Representatives _____

7. *a* Nature of the proceedings (divorce, paternity, breach of contract, product liability, etc.) (article 3,c) _____
- b* Summary of complaint _____
- c* Summary of defence and counterclaim* _____
- d* Other necessary information or documents* _____
- * Omit if not applicable.
8. *a* Evidence to be obtained or other judicial act to be performed (article 3,d) _____
- b* Purpose of the evidence or judicial act sought _____
9. Identity _____
 and
 address
 of any
 person to
 be examined
 d
 (article
 3,e)*
10. Questions _____
 to be
 put to
 the
 persons
 to be
 examined
 d or
 statement
 of the
 subject
 matter
 about
 which
 they
 are to

- be examined (article 3,f)*
11. Documents _____ or other property to be inspected (article 3,g)*
12. Any _____
 re- *(In the event that the evidence cannot be*
 quire- *taken in the manner requested, specify*
 ment *whether it is to be requested, specify*
 that *whether it is to be law for the formal tak-*
 the *ing of evidence.)*
 evid-
 ence
 be
 given
 on
 oath
 or af-
 firma-
 tion
 and
 any
 spe-
 cial
 form
 to be
 used
 (article
 3,h)*
13. Spe- _____
 cial *(In the event that the evidence cannot be*
 meth- *taken in the manner requested, specify*
 ods or *whether it is to be taken in such manner*
 pro- *as provided by local law)*
 ced-

ure to
be
fol-
lowed
(*e.g.*
oral
or in
writ-
ing,
ver-
batim,
tran-
script
or
sum-
mary,
cross-
exam-
ina-
tion,
etc.)
(articl
es 3,*i*
and
9)*

14. Re-
quest
for
noti-
fica-
tion
of the
time
and
place
for
the
exe-
cution
of the
Re-
quest
and
iden-
tity
and
ad-
dress
of any
per-
-

- son to
be no-
tified
(articl
e 7)*
15. Re- _____
quest
for at-
tend-
ance
or
parti-
cipa-
tion
of ju-
dicial
per-
son-
nel of
the re-
quest-
ing
au-
thor-
ity at
the
exe-
cution
of the
Letter
of Re-
quest
(articl
e 8)*
16. Spe- _____ (*attach copies of*
cifica- *relevant laws or regulations*)
tion
of
priv-
ilege
or
duty
to re-
fuse
to
give
evid-
ence
under

the
law of
the
State
of ori-
gin
(articl
e 11,
b)*

*

Omit
if not
ap-
plicab
le.

17. The _____ (*identity and ad-
dress*)
fees
and
costs
in-
curred
which
are re-
im-
burs-
able
under
the
secon
d
para-
graph
of art-
icle
14 or
under
article
26 of
the
Con-
ven-
tion
will
be
borne
by*

*

Omit
if not

ap-
plicab
le.

DATE OF REQUEST

SIGNATURE AND SEAL OF
THE REQUESTING AUTHORITY

NOTES:

Use of Form:

This form is an official form; the format and wording were created and approved under the Hague Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters. The wording and format should not be altered.

Authority:

Hague Convention for Evidence, Art. 1

Discussion:

See *14.12*

Related Form for Motion and Notice of Motion:

See *14.30*



139 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
VII. FORMS

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.34

AUTHOR: Diane E. Barry, Esq.

14.34 Letters Rogatory--Form A Under Additional Protocol to the Inter-American Commission on Letters Rogatory.

Letters Rogatory--Form A Under Additional Protocol to the Inter-American Commission on Letters Rogatory.

Letter Rogatoryn1	
1	2
REQUESTING JUDICIAL OR ADMINIS-	CASE
TRATIVE AUTHORITY	:
Name:	
	DOC
Address	KET
	No.:
3	4
CENTRAL AUTHORITY OF THE STATE OF	CEN
ORIGIN	TRA
Name:	L
	AU-
Address	THO
	RITY
	OF
	THE
	STAT
	E OF
	DES-
	TIN-
	ATIO
	N

	Name :
	Ad- dress
5	6
REQUESTING PARTY	COU
Name:	NSEL
	TO
Address	THE
	RE-
	QUE
	STIN
	G
	PART
	Y
	Name :
	Ad- dress
Name:	Is this per- son
Address	re- sponsi ble for costs and ex- pense s?
	☐ YES
	☐ NO
	* If not,
	☐ check in the amount of _____ is attached.
	☐ Proof of payment is attached.

* Delete if inapplicable

The Central Authority signing this letter rogatory has the honor to transmit to you in triplicate the documents listed below and, in conformity with the Protocol to the Inter-American Convention on Letters Rogatory:

* A. Requests their prompt service on:

The undersigned authority requests that service be carried out in the following manner:

* (1) In accordance with the special procedure or additional formalities that are described below, as provided for in the second paragraph of Article 10 of the above-mentioned Convention; or

* (2) By service personally on the identified addressee or, in the case of a legal entity, on its authorized agent; or

* (3) If the person or the authorized agent of the entity to be served is not found, service shall be made in accordance with the law of the State of destination.

* B. Requests the delivery of the documents listed below to the following judicial or administrative authority:

Authority: _____

* C. Requests the Central Authority of the State of destination to return to the Central Authority of the State of origin one copy of the documents listed below and attached to this letter rogatory, and an executed Certificate on the attached Form C. *

Done at _____ this _____ date of _____, 20____.

1

2

Signature and stamp of the judicial or administrative authority of the State of origin

Signature and stamp of the Central Authority of the State of origin

Title or other identification of each document to be delivered:

NOTES:

Use of Form:

This form is an official form created and approved under the Inter-American Convention on Letters Rogatory. The wording and format should not be altered.

Authority:

Second Inter-American Specialized Conference on Private International Law: Additional Protocol to the Inter-American Convention on Letters Rogatory, May 8, 1979, *18 ILM 1238*;
<http://www.oas.org/juridico/english/treaties/b-46.html>.

Discussion:

See 14.17[3]

Related Form B for Essential Information for Addressee:

See 14.35

Related Form C for Certificate of Execution:

See 14.36

Related Form for Notice of Motion in California Court:

See 14.30

FOOTNOTES:

(n1)Footnote 1. Complete the original and two copies of this form. If A(1) is applicable, attach the original and two copies of the translation of this item in the language of the State of destination.



140 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
VII. FORMS

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.35

AUTHOR: Diane E. Barry, Esq.

14.35 Essential Information for the Addressee--Form B Under Additional Protocol to the Inter-American Commission on Letters Rogatory.

Essential Information for the Addressee--Form B Under Additional Protocol to the Inter-American Commission on Letters Rogatory.

ESSENTIAL INFORMATION FOR THE ADDRESSEE

To (Name and address of the person being served):

.....

You are hereby informed that (Brief statement of nature of service):

.....

A copy of the letter rogatory that gives rise to the service or delivery of these documents is attached to this document. This copy also contains essential information for you. Also attached are copies of the complaint or pleading initiating the action in which the letter rogatory was issued, of the documents attached to the complaint or pleading, and of any rulings that ordered the issuance of the letter rogatory.

ADDITIONAL INFORMATION

I *

FOR SERVICE

A. The document being served on you (original or copy) concerns the following:

B. The remedies sought or the amount in dispute is as follows:

C. By this service, you are requested:

* D. In case of service on you as a defendant you can answer the complaint before the judicial or administrative authority specified in Form A, Box 1 (State place, date and hour):

* You are being summoned to appear as: _____

* If some other action is being requested of the person served, please describe: _____

E. If you fail to comply, the consequences might be: _____

F. You are hereby informed that a defense counsel appointed by the Court or the following legal aid societies are available to you at the place where the proceeding is pending.

Name:

Address:

The documents listed in Part III are being furnished to you so that you may better understand and defend your interests.

II *

FOR INFORMATION FROM JUDICIAL OR ADMINISTRATIVE AUTHORITY

To: (Name and address of the judicial or administrative authority)

You are respectfully requested to furnish the undersigned judicial or administrative authority with the following information: _____

The documents listed in Part III are being furnished to you to facilitate your reply.

** Delete if inapplicable*

III

LIST OF ATTACHED DOCUMENTS

(Attach additional pages if necessary.)

(Attach additional pages if necessary.)

Done at _____ this _____ date of _____ , 20_____ .

1

Signature and stamp of the judicial or administrative authority of the State of origin

2

Signature and stamp of the Central Authority of the State of origin

NOTES:

Use of Form:

This form is an official form created and approved under the Inter-American Convention on Letters Rogatory. The wording and format should not be altered.

Authority:

Second Inter-American Specialized Conference on Private International Law: Additional Protocol to the Inter-American Convention on Letters Rogatory, May 8, 1979, *18 ILM 1238*;
<http://www.oas.org/juridico/english/treaties/b-46.html>

Discussion:

See 14.17[3]

Related Form A for Letters Rogatory:

See 14.34

Related Form C for Certificate of Execution:

See 14.36

Related Form for Notice of Motion in California Court:

See 14.30



141 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 14 Discovery of Electronically Stored Information Residing in Foreign Jurisdictions
VII. FORMS

1-14 MB Practice Guide: CA E-Discovery and Evidence 14.36

AUTHOR: Diane E. Barry, Esq.

14.36 Certificate of Execution--Form C Pursuant to Additional Protocol to the Inter-American Convention on Letters Rogatory

Certificate of Execution--Form C Pursuant to Additional Protocol to the Inter-American Convention on Letters Rogatory

CERTIFICATE OF EXECUTION

To: _____

(Name and address of judicial or administrative authority that issued the letter rogatory)

In conformity with the Additional Protocol to the Inter-American Convention on Letters Rogatory, signed at Montevideo on May 8, 1979, and in accordance with the attached original letter rogatory, the undersigned Central Authority has the honor to certify the following:

* A. That one copy of the documents attached to this Certificate has been served or delivered as follows:

Date:

At (Address): _____

By one of the following methods authorized by the Convention.

* (1) In accordance with the special procedure or additional formalities that are described below, as provided for in the

second paragraph of Article 10 of the above-mentioned Convention, or

* (2) By service personally on the identified addressee or, in the case of a legal entity, on its authorized agent, or

* (3) If the person or the authorized agent of the entity to be served was not found, in accordance with the law of the State of destination: (Specify method used)

* B. That the documents referred to in the letter rogatory have been delivered to:

Identity of person:

Relationship to the addressee: (family, business or other)

* C. That the documents attached to the Certificate have not been served or delivered for the following reason(s):

* D. In conformity with the Protocol, the party requesting execution of the letter rogatory is requested to pay the outstanding balance of costs in the amount indicated in the attached statement. *

Done at _____ this _____ date of _____, 20____.

_____ Signature and stamp of Central Authority of the State of destination

Where appropriate, attach originals or copies of any additional documents proving service or delivery, and identify them.

* *Delete if inapplicable*

NOTES:

Use of Form:

This form is an official form created and approved under the Inter-American Convention on Letters Rogatory. The wording and format should not be altered.

Authority:

Second Inter-American Specialized Conference on Private International Law: Additional Protocol to the Inter-American Convention on Letters Rogatory, May 8, 1979, *18 ILM 1238*;
<http://www.oas.org/juridico/english/treaties/b-46.html>.

Discussion:

See *14.17[3]*

Related Form A for Letters Rogatory:

See *14.34*

Related Form B for Essential Information for Addressee:

See *14.35*

Related Form for Notice of Motion in California Court:

See *14.30*



142 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.syn

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

§ 15.syn Synopsis to Chapter 15: Admissibility of Electronic Evidence at Trial

15.01 Scope.

15.02 Objective and Strategy.

15.03 CHECKLIST: General Requirements for ESI Admissibility

15.04 Options and Strategy.

15.05 General Rules of Admissibility Apply to ESI.

15.05[1] For Evidence Purposes, ESI Is a "Writing."

15.05[2] ESI Must Meet Criteria for Admissibility.

15.05[2][a] ESI Must Meet Five Basic Criteria for Admission Into Evidence.

15.05[2][b] ESI Must Be Relevant.

15.05[2][c] ESI Must Be Authentic.

15.05[2][d] ESI Must Not Include Impermissible Hearsay.

15.05[2][e] ESI Must Constitute an Original (or an Acceptable Copy).

15.05[2][f] ESI Must Not Be Unfairly Prejudicial.

15.06 Court's Decisions Regarding Admissibility Will Be Reviewed Only for Abuse of Discretion.

15.07 ESI Practice Has Particular Concerns When Considering Authenticity, Hearsay Exceptions, and Original/Duplicate Copies.

15.07[1] Areas of Particular Concern With ESI.

15.07[2] Authenticity Issues.

15.07[3] Issues Involving Hearsay Exceptions.

15.07[4] Issues Involving Secondary Evidence Rule.

15.08 Most Evidence Is Admitted Through Stipulation.

15.09 Counsel Must Be Prepared to Prove Admissibility.

15.09[1] Counsel Should Have a Fallback Position in Case Other Side Will Not Stipulate.

15.09[2] Collection of Fallback Foundational Information Should Begin Early in Discovery.

15.10 CHECKLIST: Establishing or Attacking the Authenticity of ESI Evidence.

15.11 Options and Strategy.

15.12 Counsel Must Show That Writing Is What Proponent Says It Is.

15.13 Documents Claimed to Be Forged or Falsified Must Be Authenticated As Such.

15.14 Counsel Need Only Make a Prima Facie Showing of Authenticity.

15.15 Evid Code § 1410 et seq. Provide Standard Methods of Proving Authenticity.

15.15[1] Statutory Methods Provide a Starting Point.

15.15[2] ESI May Be Authenticated by Witness to Its "Execution."

15.15[3] ESI May Be Authenticated by Party Opponent's Admission of Authenticity.

15.15[4] ESI May Be Authenticated by Evidence That It Is Reply to Communication Sent to Author.

15.15[5] ESI May Be Authenticated by Content of Facts Unlikely to Be Known to Anyone Other Than Purported Author.

15.15[6] ESI May Be Authenticated by Other Indicia of Authenticity.

15.16 Additional Methods of Authentication Are Particular to ESI Evidence.

15.16[1] Custodian/Source, and File/Path Information May Be Used to Authenticate ESI.

15.16[2] Metadata May Be Used to Authenticate ESI.

15.16[3] System Logs May Be Used to Authenticate ESI.

15.16[4] Network Security Information May Be Used to Authenticate ESI.

15.17 Counsel Also May Use ESI Data to Attack ESI Authenticity.

15.17[1] Some Methods of Attacking Authenticity Are Specific to ESI.

15.17[2] Source/Custodian and File/Path Information May Be Used to Attack ESI Authenticity.

15.17[3] Metadata May Be Used to Attack ESI Authenticity.

15.17[4] Authenticity of ESI May Be Attacked by Attacking Collecting Tools and/or Collecting Technician.

15.17[5] Authenticity of ESI May Be Attacked by Showing Faulty Chain of Custody.

15.17[6] Evidence of Processing and Manipulation May Be Used to Attack ESI Authenticity.

15.18 Expert Assistance Is Essential for Establishing or Attacking ESI Technical Authenticity.

15.19 CHECKLIST: Applying the Hearsay Rule and Its Exceptions to ESI

15.20 Options and Strategy.

15.21 Hearsay Is Defined by Statute.

15.22 Computer Generated Information May Not Be Hearsay.

15.23 Hearsay Is Inadmissible Except As Otherwise Permitted by Law.

15.23[1] General Rule Is That Hearsay Is Inadmissible.

15.23[2] Hearsay Is Admissible If Sufficiently Trustworthy.

15.24 Hearsay Is Admissible If It Falls Within an Exception to General Rule.

15.24[1] California Statutes Provide Numerous Hearsay Exceptions.

15.24[2] Nonstatutory "Catch All" Hearsay Exception Exists for "Other Indicia of Trustworthiness."

15.25 ESI May Be Admissible Under Business Records Exception to the Hearsay Rule.

15.25[1] Business Records Are Admissible Hearsay.

15.25[2] Statutory Definition of "Business" Includes Governments and Nonprofits.

15.25[3] Court Has Discretion Regarding Qualification As Business Record.

15.25[4] ESI Must Have Been Prepared in the "Ordinary Course of Business."

15.25[5] ESI Must Have Been Created at or Near the Timing of Act, Condition, or Event.

15.25[6] Custodian Must Testify Regarding Identity and Methods of Preparation.

15.25[7] Custodian Need Not Testify That Computer Is Reliable.

15.25[8] Testimony Must Show Trustworthiness.

15.26 ESI May Be Admissible Under the Official Records Exception to the Hearsay Rule.

15.26[1] Official Records Exception Applies to Records Made by Public Employees.

15.26[2] ESI Must Have Been Prepared by a Public Employee Acting Within the Scope of Duty.

15.26[2][a] "Public Employee" Is Broadly Defined.

15.26[2][b] Public Employee Must Create Rather Than Simply Accept or Store Data.

15.26[2][c] ESI Must Be Within Mandate of Agency's or Employee's Duties.

15.26[3] ESI Must Have Been Made at or Near the Time of Act, Condition, or Event.

15.26[4] Sources, Methodology, and Timing Must Indicate Trustworthiness.

15.26[4][a] Trustworthiness Must Be Shown.

15.26[4][b] Trustworthiness May Be Proved Without Witness Testimony.

15.26[4][c] Trustworthiness May Be Proved by Judicial Notice.

15.26[4][d] Proffering Party May Invoke Presumption That an Official Duty Was Regularly Performed.

15.27 ESI May Be Admissible Under Catch All Hearsay Exception by Showing Other Indicia of Trustworthiness.

15.28 CHECKLIST: Applying the Secondary Evidence Rule to ESI

15.29 Options and Strategy.

15.30 Content of Writing May Be Proved by Otherwise Admissible Original.

15.30[1] Content of Writing May Be Proved by Original in All Cases.

15.30[2] Content of Writing Must Still Be Proved by Original in Some Cases.

15.30[3] Computer Printout or Other Similar Output Qualifies As an "Original."

15.30[4] Computer Printout Is Presumed to Accurately Reflect System Data.

15.31 Content of Writing May Be Proved by Otherwise Admissible Secondary Evidence in Most Cases.

15.31[1] Secondary Evidence Generally May Be Used to Prove Content of Writing.

15.31[2] Court Must Exclude Secondary Evidence of Writing Under Specified Circumstances.

15.32 Content of Writing May Be Proved by Oral Testimony Under Limited Circumstances.

15.33 Stipulation Regarding Admission of Items of ESI Into Evidence

15.34 Chain of Custody Record for ESI.

15.35 Sample Direct Examination Questions--Authenticating an E-Mail.

15.36 Sample Direct Examination Questions--Authenticating an Electronic Record.

15.37 Sample Direct Examination Questions--Direct Examination Admission of Party.

Diane E. Barry, Esq. n*

Hon. James L. Smith (Ret.), n** ***Practice Consultant***

FOOTNOTES:

(n4)Footnote *. Diane E. Barry, Esq. is the Director of Discovery Strategy and Management at International Litigation Services, Inc. Diane's practice focuses on ESI discovery under state and federal rules of civil procedure, and complex litigation discovery planning and management. Diane assists clients in planning and preparing for ESI discovery conferences and court appearances, as well as preparation for specialized discovery such as IT custodian depositions, key player and IT interviews. In addition, Diane has significant expertise in utilizing technology to improve results in privilege and relevance review. Diane is earned her A.B. degree from Vassar College and her J.D. degree, cum laude, from the Boston University School of Law. She holds a professional certification in Data Warehousing from U.C. Berkeley.

(n5)Footnote **. Hon. James L. Smith (Ret.) is an arbitrator and mediator for JAMS in Orange, CA. He has over 38 years of experience in resolving disputes, both as a trial court judge and an independent mediator, arbitrator, special master, and discovery referee in both federal and state court litigation. As a trial judge for over 26 years, he presided over thousands of cases, many of which were complex litigation matters involving business/commercial issues. To this day, Judge Smith is the only Orange County Judge, active or retired, to have been assigned to all of the Court's calendars, including two years as Presiding Judge of the Court, two years as Supervising Judge of the Criminal Panel, and two years as Presiding Judge of the Probate Department. In addition Judge Smith served in various assignments including Family Law, Juvenile Court, Mental Health, Complex Litigation, Civil Panel, Criminal Panel and Mandatory Settlement Calendar. He also has handled a wide variety of cases from e-discovery and intellectual property to personal injury and trusts and estates. Judge Smith earned his J.D. from Hastings College of Law and his B.A. from the University of Redlands



143 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial

I. STRATEGY

3-15 MB Practice Guide: CA E-Discovery and Evidence 15.01

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.01 Scope.

This chapter covers the hurdles that must be met in order to get electronically stored information admitted into evidence. It focuses on issues that present particular problems and issues in the context of ESI that do not arise in other types of evidence, particularly in the areas of authentication, hearsay and the secondary evidence rule. It also covers the grounds for attacking proffered ESI evidence.

Core Statutes:

Evid Code §§ 250 (definition of a writing), 210, 350 (relevance), 1400, 1401 (authenticity); 1200, 1220-1350 (hearsay rule and exceptions), 1520 et seq. (secondary evidence rule and rules regarding originals and duplicates), 352 (exclusion of evidence due to unfair prejudice).



144 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
I. STRATEGY

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.02

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.02 Objective and Strategy.

This chapter is designed to provide counsel with guidance regarding aspects of evidence admissibility which are particular to working with ESI evidence. Therefore, this chapter will not provide a full scope primer on getting materials into evidence.

Under the California Evidence Code, ESI is essentially a writing--that is, a piece of documentary evidence [*Evid Code* § 250 (definition of a writing)]. The five threshold questions that must be overcome in order to get any documentary item into evidence are:

- Is it relevant [*Evid Code* §§ 210, 350; *Traxler v. Thompson* (1970) 4 CA3d 278, 84 CR 211 (relevant substantial evidence must support verdict)]?
- Is it authentic [*Evid Code* §§ 1400, 1401 (authenticity); *Continental Baking Co. v. Katz* (1968) 68 C2d 512, 525, 67 CR 761 (document is not presumed to be what it purports to be, and it must be authenticated before it can be introduced into evidence)]?
- Does it contain inadmissible hearsay [*Evid Code* § 1200, 1220-1350 (hearsay rule and exceptions)]?
- Best evidence concerns: is it an original or acceptable secondary document [*Evid Code* § 1520 *et seq.* (secondary evidence rule and rules regarding originals and duplicates)]?
- Should it be excluded on the grounds of unfair prejudice [*Evid Code* § 352 (exclusion of evidence due to unfair prejudice)]?

Relevance and unfair prejudice are usually case- and fact-specific, and the considerations are much the same for ESI evidence as for ordinary documentary evidence. This chapter focuses on the considerations particular to ESI evidence when considering authenticity, hearsay exceptions, and best evidence concerns.



Strategic Point: Conduct E-Discovery With Admissibility in Mind.

Proper preparation for the admission of ESI should begin in the e-discovery phase of the litigation. Counsel must make certain that the ESI is collected and preserved in a manner that will not compromise its admissibility at trial.

 Cross References:

For section-by-section discussion of the admission of evidence under the California Evidence Code, annotated with cases and expert commentary, see Cotchett, *California Courtroom Evidence* (LexisNexis).

For detailed guidance on laying proper foundations for the admission of every type of evidence in California, including scripted questions that may be used to lay the necessary foundations, see Imwinkelried & Leach, *California Evidentiary Foundations* (4th ed.) (LexisNexis).



145 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
II. GENERAL REQUIREMENTS FOR ESI ADMISSIBILITY

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.03

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.03 CHECKLIST: General Requirements for ESI Admissibility

☐ Is the ESI evidence relevant?

Authority:

Evid Code § 210; Traxler v. Thompson (1970) 4 CA3d 278, 84 CR 211

Discussion:

See 15.05[2][b]

☐ Is the ESI authentic?

Authority:

Evid Code §§ 1400, 1401; Continental Baking Co. v. Katz (1968) 68 C2d 512, 525 . 67 CR 761 ; see In Re Vinhnee (B.A.P. 9th Cir. 2005) 336 BR 437

Discussion:

See 15.05[2][c], 15.10-15.18

☐ Does the ESI contain hearsay?

Authority:

Evid Code §§ 225 (definition of "statement"), 1200 (hearsay rule), 1201 (multiple hearsay)

Discussion:

See 15.05[d], 15.19-15.27

☐ If the ESI contains hearsay, does it fit within one of the accepted hearsay exclusions?

Authority:

Evid Code §§ 1200 et seq. (hearsay rules and exceptions)

Discussion:

See 15.05[2][d]

- ☐ Is the ESI an "original" or acceptable (otherwise admissible) secondary evidence?

Authority:

Evid Code §§ 250 (definition of "writing"), 255 (definition of "original"), 1520-1523 (methods of proof for originals and copies)

Discussion:

See 15.05[2][e], 15.28-15.32

- ☐ Is the ESI unfairly prejudicial to either party in relation to the evidence's probative value?

Authority:

Evid Code § 352

Discussion:

See 15.05[f]



146 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
II. GENERAL REQUIREMENTS FOR ESI ADMISSIBILITY

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.04

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.04 Options and Strategy.

A party seeking to admit ESI into evidence, or to oppose its admission, should review the basic criteria for admission of *all* documentary evidence, make certain that each issue is considered with respect to the ESI in question, and identify the criteria that are most likely to be problematic. This Part covers the basic criteria for admissibility as they apply to ESI evidence, and identifies evidentiary concerns which are particular to ESI practice.



147 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
II. GENERAL REQUIREMENTS FOR ESI ADMISSIBILITY

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.05

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.05 General Rules of Admissibility Apply to ESI.

15.05[1] For Evidence Purposes, ESI Is a "Writing." *Evid Code § 250* defines a "writings" to include "handwriting, typewriting, printing, photostating, photographing, photocopying, transmitting by electronic mail or facsimile, and every other means of recording upon any tangible thing, any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combinations thereof, and any record thereby created, regardless of the manner in which the record has been stored." Therefore, for purposes of offering a piece of ESI into evidence, ESI is a "writing" and the general rules of evidence for documentary items apply [*Evid Code §§ 250, 255, 1520-1523, see, e.g. Jones v. City of Los Angeles* (1993) 20 CA4th 436, 24 CR2d 528 (applying admission standards for "writing" to videotape)].

15.05[2] ESI Must Meet Criteria for Admissibility.

15.05[2][a] ESI Must Meet Five Basic Criteria for Admission Into Evidence. When offering a piece of ESI into evidence, counsel must be prepared to show that it:

- Is relevant.
- Is authentic.
- Does not contain impermissible hearsay.
- Is "original," or is otherwise admissible secondary evidence.
- Is not unduly prejudicial.

Examples--Application of General Rules of Evidence Admissibility to ESI:

- In an auto accident case, the plaintiff paralegic submitted for admission into evidence a 20 minute

videotape depicting an average day in her life since her accident. The defendant city objected on the grounds that the tape was irrelevant, unauthentic, hearsay, cumulative, and prejudicial. The trial court admitted the tape into evidence, and admission was upheld on appeal. The Second District stated that the tape was a "writing" within the meaning of the Evidence Code and therefore must comply with the admissibility requirements for writings; that the tape was relevant as to what plaintiff's treatment and daily activities were; that the plaintiff's testimony stating that the film was accurate satisfied the authenticity requirement; and that this proof of her actual injuries was not unduly prejudicial. Introduction of the tape into evidence was not an abuse of the trial court's discretion [*Jones v City of Los Angeles* (2nd Dist. 1993) 20 CA4th 436 ; 24 CR2d 528] .

■ The DMV, in an administrative hearing, suspended the plaintiff's driver's license for driving with a blood alcohol level in excess of .08, the level at which one's driving is presumed to be impaired. On appeal to the superior court, the suspension was dismissed. The superior court held that no admissible evidence of plaintiff's blood alcohol level had been presented at the hearing. The primary contentions pertained to a DMV computerized printout of a lab report which purported to show that plaintiff's blood alcohol level had been at an unacceptable level. The lab report containing the results of the blood alcohol testing was prepared 8 days after the initial blood test was performed. The DMV claimed the report was an acceptable computerized printout of a government record, admissible despite hearsay considerations under *Veh Code* § 23612(g)(2). The superior court excluded it as inadmissible hearsay, finding that the report had not been created "at or near" the time when the blood test had been performed, as required for records of an act or condition under *Evid Code* § 1280. On appeal, the Sixth District upheld the exclusion. Since the underlying lab report was not admissible, the computer printout of it was not admissible, and there was no acceptable evidence supporting a finding of the requisite blood alcohol level [*Molenda v. DMV* (2009) 172 CA4th 974 ; 91 CR3d 792 ; but see *Komizu v. Gourley* (2002), 103 CA4th 1001, 127 CR2d 229 (report of appellant's blood alcohol content typed six days after appellant's blood was analyzed was properly admitted into evidence as it was recorded on or near the event as required by *Evid Code* § 1280)].

► Cross References:

For a general discussion of admissibility, see *California Trial Guide*, § 22.20 (Matthew Bender); see also Imwinkelried & Leach, *California Evidentiary Foundations* (4th Ed.) (LexisNexis).

15.05[2][b] ESI Must Be Relevant. ESI evidence is relevant if it has "any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence." This is a factual inquiry, and depends largely on the nature of the case at issue. Relevance concerns are likely to be the same whether the evidence being offered is ESI or another form of evidence [see *Evid Code* § 210; *Walker v. Countrywide Home Loans, Inc.* (2nd Dist. 2002) 98 CA4th 1158, 1169, 121 CR2d 79, 86 (trial court's evidentiary rulings are reviewed for abuse of discretion only)].

► Cross Reference:

Showing relevance in admission of evidence, see Cotchett, *California Courtroom Evidence* (LexisNexis), Ch. 6, Relevancy; *California Trial Guide*, Div. 4, Unit 22, Rules Affecting Admissibility of Evidence, §§ 22.20-22.30.

15.05[2][c] ESI Must Be Authentic. The proponent of the ESI must show that it is "authentic"--that it is what the proponent says it is [*Evid Code* § 1400]. A document is not presumed to be what it purports to be, and it must be authenticated before it can be introduced into evidence [*Evid Code* § 1401; *Continental Baking Co. v. Katz* (1968) 68 C2d 512, 525, 67 CR 761 ; *People v. Lugashi* (1988) 205 CA3d 632, 640, 252 CR 434 (bank's computer records were properly admitted as business record despite lack of foundational testimony as to how the computer system worked); *Aguimatang v. Cal. State Lottery* (1991) 234 CA3d 769, 805, 286 CR 57 (computer printout of lottery winners was

admissible in dispute about whether a fourth missing lottery ticket was ever issued; proper foundation as to computer records was established by lottery manager)].

➤ **Cross Reference:**

Authentication of ESI evidence, see 15.10-15.18.

15.05[2][d] ESI Must Not Include Impermissible Hearsay. The Evidence Code defines hearsay as a statement made by someone other than the witness who is testifying, which is being offered to prove the truth of the matter stated. In order to be admissible, either the ESI must not contain any such hearsay, or it must fit within at least one of the recognized hearsay exceptions [*Evid Code* §§ 1200 (hearsay rule), 1201 (multiple hearsay), 1220 et seq. (hearsay exceptions); *Molenda v. DMV* (2009) 172 CA4th 974 ; 91 CR3d 792 (computerized printout of lab report excluded as impermissible hearsay); *People v. Lugashi* (1988) 205 CA3d 632, 640, 252 CR 434 (bank's computer records were properly admitted under business record exception to hearsay rule despite lack of foundational testimony as to how the computer system worked)].

➤ **Cross Reference:**

Hearsay issues in ESI evidence, see 15.19-15.27.

15.05[2][e] ESI Must Constitute an Original (or an Acceptable Copy). California replaced the traditional "best evidence rule" with the "secondary evidence rule" in 1999. Under this approach, the contents of a writing may be proved either through an original or "otherwise admissible secondary evidence" [*Evid Code* §§ 1520, 1521]. Otherwise admissible secondary evidence is just as acceptable as the original, unless either (1) a genuine dispute exists concerning the material terms of the writing and justice requires the exclusion; or (2) admission of the secondary evidence would be unfair [*Evid Code* §§ 1520, 1521; *Osswald v. Anderson* (1996) 49 CA4th 812, 57 CR2d 23 (genuine dispute existed as to terms of trust writing, invalidating proof of contents of writing by secondary means)]. *Evid Code* §§ 1552 and 1553 establish presumptions that printouts of information or images from a computer are presumed to be an accurate representation of the computer information or computer program that it purports to represent.

➤ **Cross Reference:**

Applying the secondary evidence rule to ESI, 15.28-15.32.

15.05[2][f] ESI Must Not Be Unfairly Prejudicial. The trial court has discretion to exclude otherwise admissible evidence if it would create a substantial danger of jury confusion or undue prejudice. Like considerations of relevance, this is largely a factual inquiry and is considered on a case by case basis. It will depend on the nature of the ESI evidence and the context in which it is being offered. Prejudice and confusion concerns are likely to be the same regardless of the form of the evidence being presented [*Evid Code* § 352; *People v. Durham* (1969) 70 C2d 171, 74 CR 262, 449 P2d 198 (allegedly inflammatory evidence is admissible only when its probative value outweighs its prejudicial effect); *Huber, Hunt & Nichols, Inc. v. Moore* (1977) 67 CA3d 278, 296-297, 136 CR 603 (trial court properly excluded lengthy and complex computer printout of costs that would be incomprehensible to lay juror, and would be unduly prejudicial and confusing because costs caused by wrongful acts were not segregated)].

➤ **Cross Reference:**

California Trial Guide (LexisNexis), Div. 4, Unit 22, Rules Affecting Admissibility of Evidence, §§ 22.40-22.50.



148 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
II. GENERAL REQUIREMENTS FOR ESI ADMISSIBILITY

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.06

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.06 Court's Decisions Regarding Admissibility Will Be Reviewed Only for Abuse of Discretion.

Courts are vested with broad discretion to decide admission issues, including authenticity. The trial court's decisions which pertain to the admissibility of evidence will be reviewed for abuse of discretion only [*see, e.g., People v. Minifie* (1996) 13 C4th 1055, 1069-1070, 56 CR2d 133, 920 P2d 1337 (trial court's decision to exclude evidence as prejudicial will not be overturned absent an abuse of that discretion.); *Jones v. City of Los Angeles* (1993) 20 CA4th 436, 24 CR2d 528 (applying an abuse of discretion standard and upholding trial court's decision to admit a videotape as authentic)].



149 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
II. GENERAL REQUIREMENTS FOR ESI ADMISSIBILITY

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.07

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.07 ESI Practice Has Particular Concerns When Considering Authenticity, Hearsay Exceptions, and Original/Duplicate Copies.

15.07[1] Areas of Particular Concern With ESI. The primary issues in which admissibility of ESI evidence can differ greatly from the admissibility of paper writings are:

- Authenticity.
- Hearsay exceptions.
- What is an original/duplicate?

► **Cross References:**

Authentication of ESI evidence, see 15.10-15.18.

Hearsay issues in ESI evidence, see 15.19-15.27.

Applying the secondary evidence rule to ESI, 15.28-15.32.

15.07[2] Authenticity Issues. The following issues authenticity issues are of particular concern when considering ESI:

- How does everyone know that this computer data is what the proponent says it is?
- How does everyone know that it is Ms. X's e-mail, or that it is Mr. Y's PowerPoint document?

ESI has considerable information available that does not exist in the case of paper documents.

► **Cross Reference:**

Detailed discussion of addressing authenticity issues involving ESI, see *15.10-15.18*.

15.07[3] Issues Involving Hearsay Exceptions. Hearsay exceptions usually provide for an exception when the information can be proved to be otherwise reliable. The problem counsel faces with ESI is how reliability can be shown for computer records.

Examples:

- Businesses use computer programs and systems for all kinds of business purposes and rely upon these systems to help them make important decisions and to perform critical business functions. Counsel must consider what kind of proof will show that a computer database is an acceptable business record.
- A human relations file may purport to show a particular employee's history with the company, all the way to the termination of employment. The employee was fired in reliance on this record. Counsel must determine how to get it into evidence.

 Cross Reference:

Detailed discussion of applying hearsay exceptions to ESI records, see *15.19-15.27*.

15.07[4] Issues Involving Secondary Evidence Rule. One problem with ESI is that the data may never have been printed out. Most users read e-mail, respond to its contents, and delete it without ever printing it out. Information is entered into accounting systems--invoices go in; payments go out; the entries are processed and responded to without ever becoming "hard copies." These "writings" may never have had any physical form. Counsel is presented with an issue regarding what constitutes an "original" of something that has never had physical existence, and in what form to introduce the ESI into evidence.

 Cross Reference:

Application of secondary evidence rule to ESI, see *15.28-15.32*.



150 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
 II. GENERAL REQUIREMENTS FOR ESI ADMISSIBILITY

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.08

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant**15.08 Most Evidence Is Admitted Through Stipulation.**

The usual method for getting any item into evidence is through stipulation among the parties. The stipulation can agree to full admission of the ESI, or it can stipulate to any of the threshold findings discussed below required for admission [CCP §§ 281(1) (authority of counsel to bind clients), 2023.010(i) (failure to meet and confer in good faith is a sanctionable discovery abuse); *County of Alameda v. Risby* (1994) 28 CA4th 1425, 1430, 34 CR2d 333 (parties may stipulate to admission of otherwise inadmissible evidence); *Lorraine v. Markel* (D Md 2007) 241 FRD 534 (discussion under FRCP of procedures for parties to stipulate to authenticity of ESI evidence)].

 Cross Reference:

Sample form for stipulation to admission of ESI evidence, 15.33.

**Warning:**

Stipulations pertaining to the admission of evidence, absent an express limitation, apply to a later trial of the same action, unless the trial court allows the stipulation to be withdrawn [*City of Hope National Medical Center v. Genentech, Inc.* (2008) 43 C4th 375, 398, 75 CR3d 333, 181 P3d 142 (stipulation admitted after withdrawal denied)].

**Strategic Points:**

- If opposing counsel refuses to stipulate to the authenticity of an item when there are no grounds to question its authenticity, counsel should consider drafting a request for admission, to be followed by a form interrogatory demanding identification of all facts, documents, and witnesses upon which counsel bases the refusal to agree to authenticity [CCP § 2033.010 (requests for admissions)].
- Counsel should also consider bringing a motion for discovery abuse [see CCP § 2023.010 (discovery abuse defined); *Rico v Mitsubishi Motors Corp.* (2007) 42 C4th 807, 818, 68 CR3d 758, 171 P3d 1092 ("[A]n attorney has an obligation not only to protect his client's interests but also to respect the legitimate

interests of fellow members of the bar, the judiciary, and the administration of justice"), citing *Kirsch v. Duryea* (1978) 21 C3d 303, 309, 146 CR 218, 222, 578 P2d 935] .

 Cross References:

Stipulations on evidentiary matters, see *Matthew Bender(R) Practice Guide: California Pretrial Civil Procedure*, Ch. 28, *Stipulations*, 28.08; *California Forms of Pleading and Practice*, Ch. 533, *Stipulations*, 533.13[6] (Matthew Bender).

Making requests for admissions, see *Matthew Bender(R) Practice Guide: California Civil Discovery*, Ch. 12, *Requests for Admissions*.

Requesting imposition of sanctions for misuse of discovery, see *Matthew Bender(R) Practice Guide: California Civil Discovery*, Ch. 3, *Sanctions*, 3.03 et seq.



151 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
II. GENERAL REQUIREMENTS FOR ESI ADMISSIBILITY

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.09

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.09 Counsel Must Be Prepared to Prove Admissibility.

15.09[1] Counsel Should Have a Fallback Position in Case Other Side Will Not Stipulate. Although admission by stipulation is a common practice, it is wise to remember that it will not always be possible. There may be a genuine issue of fact as to authenticity, or other reasonable grounds on which opposing parties and their counsel may refuse to stipulate to the admission of a particular piece of ESI evidence. The possibility also exists that the court will raise its own objections to evidence *sua sponte*, even when the opposition did not object [*see, e.g., Lorraine v. Markel American Ins. Co. (2007) 241 FRD 534* (court denied cross-motions for summary judgment as neither side authenticated the attached ESI evidence--no discussion of objections by the parties, only the objections of the court); *In Re Vinhnee (B.A.P. 9th Cir. 2005) 336 BR 437* (even when there was no objection from a party, bankruptcy court could insist that proffering party prove up all aspects of business records hearsay exception)].

Consider:

When there are admissibility problems, they often pertain to a particularly important piece of evidence. If the evidence were innocuous, no one would be wasting their time either seeking or opposing its admission.



Warning:

Under these circumstances, counsel always must have a fallback position ready just in case admission through stipulation is unavailable. The best laid plans can go awry. Counsel must be ready to prove the foundation necessary to admit expensive ESI evidence. Counsel should *not* rely upon the good will of opposing counsel or laxity on the part of the court.

15.09[2] Collection of Fallback Foundational Information Should Begin Early in Discovery. Foundational information regarding authenticity, appropriate hearsay exceptions and original/secondary evidence concerns must be gathered during discovery, so that a fallback position is ready. The early meeting of counsel, interrogatories, requests for admission, and deposition practice can all be used to gather the necessary foundational information for ESI, so that counsel may confidently offer this important information into evidence.

**Warning--Don't Wait Too Long:**

One of the problems attorneys experience with admissibility, and particularly with the admissibility of ESI evidence, is failing to address such concerns early in the litigation cycle. Often counsel first address admissibility at the time when they realize they would like to present a particular piece of evidence to the court. This usually occurs in connection with motions for summary judgment, or in preparation for trial. This is very late in the litigation cycle, and is often too late at that stage to fix admissibility problems. If appropriate foundational information has not been acquired prior to that time, counsel will be left scrambling to present the necessary foundational information to support admission of ESI into evidence.



152 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial

III. ESTABLISHING OR ATTACKING THE AUTHENTICITY OF ESI EVIDENCE

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.10

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.10 CHECKLIST: Establishing or Attacking the Authenticity of ESI Evidence.

☐ Contact opposing counsel and determine whether opposing counsel will stipulate to authenticity of ESI.

Authority:

CCP § 281(1) (authority of counsel to bind clients), *Continental Baking Co. v. Katz* (1968) 68 C2d 512, 525, 67 CR 761 (document is not presumed to be what it purports to be, and must be authenticated before it can be introduced into evidence); *Lorraine v. Markel* (D Md 2007) 241 FRD 534 (discussion of authenticity of ESI)

Discussion:

See 15.08

Form:

15.33

☐ If opposing counsel will not stipulate to full admission into evidence, will counsel stipulate to any threshold findings necessary for admissibility--relevance; authenticity; absence of inadmissible hearsay; fact that it is an original or acceptable secondary evidence; absence of undue prejudice?

Authority:

CCP § 281(1) (authority of counsel to bind clients); *Lorraine v. Markel* (D Md 2007) 241 FRD 534 (discussion of authenticity of ESI)

Discussion:

See 15.08

Form:

15.33

- ☐ Consider whether requests for admission can be used to compel opposing counsel to authenticate the ESI or establish any of the other threshold requirements for admissibility.

Authority:

Evid Code §§ 1400, 1401 (authenticity); *CCP § 2023.010 et seq.* (request for admissions)

Discussion:

Matthew Bender(R) Practice Guide: California Civil Discovery, Ch. 12, Requests for Admissions

- ☐ Was ESI preserved in a forensically sound manner?

Authority:

Evid Code §§ 1400, 1401 (authenticity); *Continental Baking Co. v. Katz* (1968) 68 C2d 512, 525, 67 CR 761, 439 P2d 889 (document is not presumed to be what it purports to be, and must be authenticated before it can be introduced into evidence); *Lorraine v. Markel* (D Md 2007) 241 FRD 534 (discussion of authenticity of ESI)

Discussion:

See 5.06, 9.24-9.28

- ☐ Was ESI collected in a forensically sound manner?

Authority:

Evid Code §§ 1400, 1401 (authenticity); *Continental Baking Co. v. Katz* (1968) 68 C2d 512, 525, 67 CR 761, 439 P2d 889 (document is not presumed to be what it purports to be, and must be authenticated before it can be introduced into evidence); *Lorraine v. Markel* (D Md 2007) 241 FRD 534 (Discussion of authenticity of ESI)

Discussion:

See 5.06, 9.24-9.28

- ☐ Is forensically sound source information available for this ESI?

Authority:

Evid Code §§ 1400, 1401 (authenticity); *Continental Baking Co. v. Katz* (1968) 68 C2d 512, 525, 67 CR 761, 439 P2d 889 (document is not presumed to be what it purports to be, and must be authenticated before it can be introduced into evidence); *Lorraine v. Markel* (D Md 2007) 241 FRD 534 (discussion of authenticity of ESI)

Discussion:

See 5.06, 9.24-9.28

- ☐ Is appropriate chain of custody documentation available for ESI?

Authority:

Evid Code §§ 1400, 1401 (authenticity); *Continental Baking Co. v. Katz* (1968) 68 C2d

512, 525, 67 CR 761, 439 P2d 889 (document is not presumed to be what it purports to be, and must be authenticated before it can be introduced into evidence); *Lorraine v. Markel* (D Md 2007) 241 FRD 534 (discussion of authenticity of ESI)

Discussion:

See 15.15[5]; see also 5.03 et seq, Ch. 1, Appendix A (definition of "chain of custody" and "chain of evidence")

Form:

15.34

- ☐ Has ESI been processed or altered in such a manner as to make it inadmissible?

Authority:

Evid Code §§ 1400, 1401 (authenticity); *Continental Baking Co. v. Katz* (1968) 68 C2d 512, 525, 67 CR 761, 439 P2d 889 (document is not presumed to be what it purports to be, and it must be authenticated before it can be introduced into evidence); *Lorraine v. Markel* (D Md 2007) 241 FRD 534 (discussion of authenticity of ESI)

Discussion:

See 15.17[6]; see also 5.03 et seq, Ch. 1, Appendix A (definition of "chain of custody" and "chain of evidence")

- ☐ Are appropriate witness testimony or interrogatory responses available to meet foundational authenticity requirements?

Authority:

Evid Code §§ 1400, 1401 (authenticity); *Continental Baking Co. v. Katz* (1968) 68 C2d 512, 525, 67 CR 761, 439 P2d 889 (document is not presumed to be what it purports to be, and it must be authenticated before it can be introduced into evidence); *Lorraine v. Markel* (D Md 2007) 241 FRD 534 (discussion of authenticity of ESI)); *People v. Lugashi* (1988) 205 CA3d 632, 640, 252 CR 434 (bank's computer records were properly admitted as business record despite lack of foundational testimony as to how computer system worked)

Discussion:

See Imwinkelried & Leach, California Evidentiary Foundations (4th ed.) (LexisNexis), Ch. 1, Introduction, §§ 1B, 1C.

- ☐ If target ESI system belongs to the opposition, consider taking a Person Most Knowledgeable (PMK) deposition to provide foundational information required for establishing authenticity.

Authority:

Evid Code §§ 1400, 1401 (authenticity); *CCP* §§ 2023.010(c), 2023.020 2025.250, 2025.260; 2030.010 (PMK Depositions); *Continental Baking Co. v. Katz* (1968) 68 C2d 512, 525, 67 CR 761, 439 P2d 889 (document is not presumed to be what it purports to be, and it must be authenticated before it can be introduced into evidence); *Lorraine v. Markel* (D Md 2007) 241 FRD 534 (discussion of authenticity of ESI)

Discussion:

See *15.16[1]*; see also *5A.25* et seq (deposing PMK regarding a particular ESI system)



153 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial

III. ESTABLISHING OR ATTACKING THE AUTHENTICITY OF ESI EVIDENCE

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.11

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.11 Options and Strategy.

Counsel must make a sufficient showing that ESI is authentic. Various possibilities exist for satisfying the authenticity requirement, as discussed in this part. Counsel should explore the possible ways in which the particular item of ESI evidence can be authenticated.



154 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial

III. ESTABLISHING OR ATTACKING THE AUTHENTICITY OF ESI EVIDENCE

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.12

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.12 Counsel Must Show That Writing Is What Proponent Says It Is.

Taken together, *Evid Code* §§ 1400 and 1401 require that the party offering a writing into evidence provide sufficient proof to sustain a finding that the writing is what the proponent says it is.

Consider:

Stated another way, authenticity is an extension of relevance. What does this piece of ESI need to be in order to be relevant to this matter; that is, in order to show that some aspect of the matter is more or less likely? For example: This computer printout is a printout from Partnership A's general ledger QuickBooks system. This is Ms. B's e-mail - she authored and sent it. This Word file is a draft of the minutes for the April 2010 meeting of the Board of Directors.

Therefore, in order to prove authenticity, counsel must first be able to explain *what the ESI is*, and then show the court or other trier of fact proof of *how we know that it is what counsel says it is* [*Evid Code* §§ 210, 1400, 1401; 1965 Comments of the Law Revision Committee on *Evid Code* § 1400 ("before any tangible object may be admitted into evidence, the party seeking to introduce the object must make a preliminary showing that the object is in some way relevant to the issues to be decided in the action"); *Jones v. City of Los Angeles* (1993) 20 CA4th 436, 24 CR2d 528 (proffered videotape of plaintiff paraplegic's daily activities was properly held to be authentic as it accurately showed plaintiff moving through her regular daily activities)].



Cross Reference:

Discussion of relevance, see 15.05[2][a]; see also Cotchett, California Courtroom Evidence (LexisNexis), Ch. 6, Relevancy; California Trial Guide, Div. 4, Unit 22, Rules Affecting Admissibility of Evidence, §§ 22.20-22.30.

Basic script questions for authenticating an e-mail, see 15.35.

Basic script questions for authenticating an electronic record, see 15.36.



155 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
 III. ESTABLISHING OR ATTACKING THE AUTHENTICITY OF ESI EVIDENCE

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.13

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.13 Documents Claimed to Be Forged or Falsified Must Be Authenticated As Such.

In some circumstances, "authentication" can require that counsel establish that an item is a forgery [*see Evid Code § 1402* (authentication of altered writing)].

Example:

An employee alleged that her former boyfriend, the company's CEO, had ordered her fired after she refused to have sex with him. It was undisputed that she had been fired five days after their last date. She settled the suit in 1995 for \$100,000. A key piece of evidence in that matter was a 1993 e-mail from her supervisor to the CEO confirming that he had terminated her at the latter's request. The supervisor denied that he had ever sent the e-mail. E-mail metadata, combined with cell phone records, showed the true story. The time stamp contained in the e-mail established when it was sent, and the supervisor's cell phone records, substantiated the supervisor's claim that he was traveling in his car at the precise time the e-mail was sent. The employee knew her supervisor's passwords. She broke into his e-mail account while he was out and sent the e-mail herself. Eventually, she was criminally charged and found guilty of forgery and falsification of evidence.

Under these circumstances the proponent of the e-mail is challenging authenticity and attempting to show it to be a forgery. "Authentication" in this context might consist of proving that the email in question was forged--that it was sent by someone other than the apparent sender, and in particular (if such proof is available), was sent by the accused employee. The party seeking admission of what it contends is a forged e-mail might offer testimony of the supervisor establishing that the employee knew the supervisor's login name and password; testimony of co-workers who saw the employee on a computer at a time when the forged e-mail was created and sent; testimony of the system administrator showing logs of who was logged in at critical times; testimony of the system administrator establishing that someone had logged into the account at a time when it could not have been the supervisor. Such evidence could provide the required *prima facie* showing that the item is what the proponent says it is--a forged document.



156 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial

III. ESTABLISHING OR ATTACKING THE AUTHENTICITY OF ESI EVIDENCE

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.14

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.14 Counsel Need Only Make a Prima Facie Showing of Authenticity.

In order to satisfy the authenticity requirement, the proffering party need present only a prima facie case for authenticity. Authenticity need not be proved beyond a reasonable doubt or even with a preponderance of evidence. The proffering party is only required to provide some evidence sufficient to support a finding by a reasonable person (jury) that the item is authentic. The court itself need not arrive at the conclusion that the item is authentic, only that evidence has been submitted that a reasonable jury could legally reach such a conclusion [*Verzan v. McGregor* (1863) 23 C 339, 342-343] .



157 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
 III. ESTABLISHING OR ATTACKING THE AUTHENTICITY OF ESI EVIDENCE

*1-15 MB Practice Guide: CA E-Discovery and Evidence 15.15***AUTHOR:** Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant**15.15 Evid Code § 1410 et seq. Provide Standard Methods of Proving Authenticity.**

15.15[1] Statutory Methods Provide a Starting Point. Authentication can be proved many ways. As a place to start, *Evid Code § 1410 et seq.* provide a list of tried and true means of proving authenticity. These methods have been litigated often enough that courts are comfortable that they provide reliable results. They have been granted the stature of recognized exceptions and elevated to statutory rules. Some of the statutory methods do not really apply to ESI, such as recognizing graffiti as a writing [*Evid Code § 1410.5*] and comparisons of physical handwriting [*Evid Code §§ 1415-1419*]. However, others do work well for authenticating ESI, although ESI may present special issues. Sections 15.15[2]-15.15[5] identify those statutory methods of authentication that are likely to have particular application to ESI.

**Strategic Point:**

Evid Code § 1410 et seq may not be construed to limit the means by which a writing may be authenticated or proved [*Evid Code § 1410*]. Thus, these sections provide only a starting point, not the exclusive means for authenticating ESI or any other evidence.

15.15[2] ESI May Be Authenticated by Witness to Its "Execution." Anyone who sees a "writing" being executed, including the person who wrote and/or signed it, can authenticate it [*Evid Code § 1413*]. This section can often be applied to ESI. For example, if a witness saw someone draft and send an e-mail, the proponent's counsel can argue that it was "executed" in the witness' presence.

In addition, digital signatures are legally binding to execute many kinds of documents in California [*CC §§ 1633* (digital signatures and broker/dealer contracts), 1633.1 et. seq. (Uniform Electronic Transactions Act); *Gov Code § 16.5* (digital signatures)], as well as in transactions affecting interstate or foreign commerce [*see 15 USC § 7001 et seq.* (federal Electronic Signatures in Global and National Commerce Act (E-SIGN))]. Thus, someone who saw a digital signature being generated and affixed witnessed the "execution" of the document.

**Cross Reference:**

Detailed discussion of the validity of electronic signatures under California and federal laws, see

California Forms of Pleading and Practice, Ch. 140, Contracts, § 140.26.

15.15[3] ESI May Be Authenticated by Party Opponent's Admission of Authenticity. If a party opponent has ever admitted the authenticity of an item, or shown by conduct or otherwise that the party relied upon the item--that is, showed that the party believed it to be authentic--the item can be deemed authentic. Evidence of the admission or reliance can be offered to establish authenticity [*Evid Code § 1414*].



Strategic Point:

Essentially, proffering counsel is looking for testimony or conduct that shows, for example, that a particular piece of ESI is the general ledger system the other side relied on to create its balance statements in 2009, or that a senior executive set up the meeting requested in a particular e-mail because he or she understood that the anonymous hotmail address belonged to the CEO.

Examples:

- When buyers used truck delivery weight records for calculations as to price and money owed, those records were deemed authenticated by admission through this conduct [*Jazayeri v. Mao (2009) 174 CA4th 301, 94 CR3d 198*] .
- When a company relied on a computer system in conducting its business, its conduct showed that the records from the system were sufficiently accurate to be considered authentic [see *U-Haul Int'l, Inc. v. Lumbermens Mut. Cas. Co. (9th Cir. 2009) 576 F3d 1040, 1045*] .



Cross Reference:

Script for sample direct examination questions eliciting direct examination admission of party, see 15.37.

15.15[4] ESI May Be Authenticated by Evidence That It Is Reply to Communication Sent to Author. A writing may be authenticated by evidence that the writing was received in response to a communication sent to the person who is claimed by the proponent of the evidence to be the author of the writing [*Evid Code § 1420*].

In a paper world, this exception is usually applied to correspondence.

Example--Paper Correspondence:

Mr. A sent a letter asking for information. Ms. X (who may or may not have been the addressee in the request letter) sends a letter which does not say explicitly that it is a response, but is dated two days after the request and provides most of the information demanded in the earlier letter.

In electronic correspondence, this exception works well to authenticate emails when the response comes from an open email address--that is, an anonymous account at a large commercial internet service provider. The easiest situation is when the unknown address replies and *the original email is included in the body of the reply email*. However, even when the reply comes in the form of a new email from an unknown email address, if it is dated later in time and sends the information requested, *Evid Code § 1420* authorizes authentication. Essentially, the rule allows the trier of fact to assume that the email was sent by someone who was responding to the earlier known email.

15.15[5] ESI May Be Authenticated by Content of Facts Unlikely to Be Known to Anyone Other Than Purported Author. If a piece of ESI references or reflects information that is unlikely to be known by anyone other than the person claimed as the author of the writing, these facts can establish authenticity. With regard to ESI, this section arises most often in the context of e-mail or word processing documents [*Evid Code § 1421*].

Example--Content Known Only to a Few Persons:

The author of this chapter is familiar with one situation in which a particular internet e-mail box was anonymous. Although the ISP responsible for the box was sent a third party subpoena, the information received in response was a mixture of things clearly false and things that were not particularly illuminating. During depositions, no one would admit to setting up the e-mail box, no one admitted logging into it, no one admitted knowing that it existed, and none of the work computers checked showed activity logging into that e-mail site. However, the subject matter of one of the e-mails was a corporate decision which had been known to only two persons at the opponent corporation at the time the e-mail was created and sent. There were other indications in the particular e-mail string showing that the e-mail author had been at a particular recent board of directors meeting. Both of the executives who knew about the decision had attended that meeting. Although it could not be proven which one of the two was the e-mail author, the judge admitted the item into evidence as authentic, in that it had clearly been written by one of two highly placed executives at the corporation.

15.15[6] ESI May Be Authenticated by Other Indicia of Authenticity. The Evidence Code states that the various methods listed in *Evid Code § 1400 et seq.* [see 15.15[2]-[5]] should not be construed to limit the ways in which a party can prove authenticity [*Evid Code § 1410*]. The sole requirement is that court must be able to find that the proponent has made a prima facie case for authenticity, that is, the proponent has offered enough information about the ESI that a reasonable jury could conclude that the evidence is authentic [see *Evid Code § 1400* (evidence of authentication must be sufficient to sustain finding that it is the writing that proponent claims it is); *Verzan v. McGregor* (1863) 23 Cal 339 (writing is admissible upon introduction of evidence sufficient to sustain a finding of authenticity)]. Creative counsel are welcome to bring other indicia of authenticity to the attention of the court, and should not limit themselves or their thinking to the methods listed in the Evidence Code [see *People v. Basuta* (2001) 94 CA4th 370, 114 CR2d 285 (trial court has wide discretion in deciding on admissibility of evidence and that discretion will not be disturbed absent clear showing of abuse); *US v. Safavian* (D DC 2006) FSupp2d 36 (discussing and applying multiple creative ways to authenticate e-mails under Federal Rules of Evidence)].

Example--Authenticating E-Mails by Multiple Methods Including Other Indicia of Authenticity:

In a federal criminal matter, the government sought to introduce approximately 260 e-mails. The defendant objected on grounds of authenticity and hearsay. Motions in limine brought the e-mails to the attention of the court. The court examined the e-mails, and pointed out multiple different ways to authenticate the e-mails. The court noted that (1) e-mail addresses, being unique and often including the name (or recognizable parts of the name) of a particular person, could authenticate; (2) the content of the e-mails showed conversations which could authenticate; and (3) their general appearance was that of the identified person's e-mails, which could authenticate; therefore, they could be admitted conditionally until later testimony or other admissible e-mails identified addresses or domains to authenticate. The court noted that most of the defendant's objections would affect the weight given the evidence by a trier of fact, and should not bar their entry into evidence [*United States v. Safavian* (D DC 2006) 435 F Supp2d 36, 41].



158 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial

III. ESTABLISHING OR ATTACKING THE AUTHENTICITY OF ESI EVIDENCE

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.16

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.16 Additional Methods of Authentication Are Particular to ESI Evidence.

15.16[1] Custodian/Source, and File/Path Information May Be Used to Authenticate ESI. When ESI has been preserved and collected in a forensically sound manner, the technician who collected it usually collects information about where the ESI originally resided. This usually includes who or what the source of the information: whose computer the ESI was stored on; which corporate server held the ESI; and similar information. The technician typically will collect file/path information for each piece of ESI and the exact location of the ESI on the source machine. This is similar to finding out, in a "bricks and mortar" office, whose file cabinet it was in, and the name of the paper file folder.

Example:

ESI is located on Mr. Z's computer, in his MY DOCUMENTS area, in a sub folder named GARBAGE. The resulting file/path information might look like this: C:/MyDocuments/Garbage/filename.doc. The fact that it was on Mr. Z's computer may be sufficient to authenticate it as his document. If not, it may work in conjunction with other available information. This evidence can be presented through the chain of custody documentation, declarations and/or testimony from the forensic collection technicians; and testimony from a Person Most Knowledgeable regarding the media used to store the information.

➡ Cross References:

Definitions of "chain of custody," "forensically sound," and "forensic copy," see Ch. 1, Understanding Electronic Evidence, Appendix A, Glossary.

Preservation of client's own ESI, see 5.03-5.08.

ESI involves issues not encountered in ordinary discovery, see 1.22.

Deposing person most knowledgeable (PMK) regarding ESI discovery responses, see Ch. 5A, Discovery Deposition Practice.

15.16[2] Metadata May Be Used to Authenticate ESI. Metadata is often sufficient to connect a particular file with a particular individual or to a particular computer. It may show a time frame--a date when the information was

created, sent, or received. It also may identify the real author of the document--who created it, or at least the computer workstation on which it was created.

Metadata is the information that a computer's operating system and software programs generate about a particular computer file to help them store, track and access the file. The particular metadata fields available are different for different kind of files. For example, the metadata for an e-mail will list the date and time it was sent. An MS EXCEL file is not sent, so the operating system doesn't have SENT data for this kind of file. However, it does probably track the last time the EXCEL file was modified.

Cross References:

Definition of "metadata," see Ch. 1, Understanding Electronic Evidence, Appendix A, Glossary.

Additional discussions of metadata, see 1.22[3], 1.24[4] (operating system metadata), 1.29[9] (e-mail metadata).



Strategic Points:

- To understand what metadata might be available for particular types of ESI, it will be necessary for counsel to consult a technical expert or technician who is knowledgeable about the kinds of metadata created by a particular operating system or computer program, or the metadata found associated with particular file types.

- Knowledgeable courts properly consider that metadata is part of the ESI requested, and does not need to be separately requested [see *Williams v. Sprint (D KS 2005) 230 FRD 640* ("when 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"); but see *Aguilar v. Immigration and Customs Enforcement Division of the U.S. Dept. of Homeland Security (SDNY 2008) 225 F.R.D. 350* (plaintiff who did not specify form of production or ask for metadata in its first request for production had to pay for defendant's costs of producing Word and PowerPoint files a second time if plaintiff wanted the metadata)]. However, to avoid problems in this area, specifically request metadata, both in formal written discovery and during the meet and confer conference.

- If metadata is not produced despite a request for it, the requesting party should promptly object to avoid waiver [*Ford Motor Co. v. Edgewood Properties (D.N.J. 2009) 257 FRD 418* (defendant waived its request for production in native format with metadata by failing to object within a reasonable time to plaintiff's rolling production in TIFF format)].

Cross References:

Preservation of client's own ESI, see 5.03-5.08.

Issues to be considered at "meet and confer" conference, see 5.14-5.21, 5.30 (checklist)

15.16[3] System Logs May Be Used to Authenticate ESI. System logs list various events that are tracked by the operating system components. These events usually are predetermined by the operating system itself. System log files may contain information about device changes, device drivers, system changes, events, operations and more. For

networks, they often keep track of who has logged in, and where.

**Strategic Points:**

System logs could be relevant in a trade secret case in which unauthorized access and copying of electronic files is alleged [see, e.g., *Covad Comms. Co. v. Revonet, Inc.* (D.D.C. 2009) 258 F.R.D. 5 (court observed that metadata about how database was used and accessed was at the "very heart of this lawsuit")].

**Warning:**

It is not standard practice for forensic collections personnel to collect system logs. If they are desirable, they should be specifically requested. System logs are extremely ephemeral--they are overwritten regularly. The operating system keeps track of entries for a short period of time (hours or days), and then overwrites them. If log files are of interest from an active system, i.e., one that is in current use as opposed to from a system backup, log files should be the subject of immediate communication, preservation, and collection.

15.16[4] Network Security Information May Be Used to Authenticate ESI. Business networks and other formal collections of interconnected computers usually have pre-set rules that govern where a user can reach in the network, and where the user can access and leave data--in other words, access rights. In many companies, there are network spaces open only to individuals (a personal network share) or particular departments (such as the accounting or human resources departments). If counsel wishes to show that particular documents are attributable to particular persons or groups of persons within an organization, counsel may need to obtain information regarding security access. In some cases, access may be limited to a very select few, or only the target individual. This kind of limited access can be sufficient to authenticate an e-file.

**Cross References:**

Discussion of operating systems and network data, see § 1.23.

Preservation of client's own ESI, see 5.03-5.08.



159 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial

III. ESTABLISHING OR ATTACKING THE AUTHENTICITY OF ESI EVIDENCE

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.17

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.17 Counsel Also May Use ESI Data to Attack ESI Authenticity.

15.17[1] Some Methods of Attacking Authenticity Are Specific to ESI. Just as the information particular to ESI data can provide information which can assist in authentication [see 15.16], counsel should look at those same sources (or to the lack of them) in order to attack ESI admissibility.

15.17[2] Source/Custodian and File/Path Information May Be Used to Attach ESI Authenticity. It is standard industry practice for the collecting technician to collect source/custodian, file/path information. If the collecting technician did not include this, counsel should point out that this was not done, and ask why not. In the absence of this information, others may have no way of knowing where the ESI came from.



Strategic Points:

- Counsel should make proffering counsel explain this shortfall, which exposes the ESI to attack as being unreliable.
- Counsel should also make sure that whatever source/custodian and file/path information was made available was indeed collected by the collections technician at the time of collecting the data, not at some subsequent time. This kind of information is extremely difficult, if not impossible, to create reliably later in time. If it was added later, examination of the methodology is crucial. Counsel must know who created the data, and that it was done properly.

15.17[3] Metadata May Be Used to Attack ESI Authenticity. If the ESI was not collected properly, the metadata is likely to be incorrect; it will not be the original metadata. This may be used as a basis for attacking the authenticity of the ESI.

Example:

If the client collected its own data using ordinary copying methods rather than forensically sound techniques, the creation dates on the resulting e-files may reflect the date when the ESI was collected, rather than the date when the file was originally created by the user who owns the file. Failure to preserve this information arguably is spoliation, particularly if the requesting party demanded in a preservation letter and/or the meet and confer that this metadata be preserved and collected in a manner to avoid alteration [see 5.09-5.13 (preservation demand), 5.14-5.21 (meet and confer process)]. Failure to produce it may well be a discovery abuse. It may also render the resulting ESI file inadmissible. Since the file has been altered from its original state, it arguably is not authentic.

Strategic Point:



If proffering counsel wishes to offer such "tainted" ESI into evidence, he or she must explain the altered metadata (and may well thereby place on the record sufficient information for spoliation sanctions). If proffering counsel does not offer it, the other side should consider asking about it formally and insisting on answers.



Cross References:

Definition of "metadata," see Ch. 1, Understanding Electronic Evidence, Appendix A, Glossary.

Additional discussions of metadata, see 1.22[3], 1.24[4] (operating system metadata), 1.29[9] (e-mail metadata).

Sanctions for spoliation of evidence, see 13.04-13.08.

15.17[4] Authenticity of ESI May Be Attacked by Attacking Collecting Tools and/or Collecting Technician. If the data was not properly collected, it is not reliable and may not be authentic. The proffering party must meet its requirement for a prima facie showing [see *Evid Code* §§ 1400, 1401(a)]. The attacking party need only show that the proffering party cannot make such a showing.



Cross Reference:

Proffering party required to make only prima facie showing of authenticity, see 15.14

In order to know that ESI is what counsel says it is, it must have been properly collected. The data should have been collected by a technician trained in forensic collections, using reliable (reasonable and repeatable) techniques and reliable (tried and litigated as reliable) collection tools. Counsel should seek to understand who collected the target ESI and what tools were used to collect it.

Strategic Point--Collection Tool:



If the collection tool is new and untried, it may not meet generally accepted scientific methods for forensic collection. For example, if the ESI was collected using untested open source data tools, it may be impossible for anyone else to know if the untried tool actually collected the data properly--in other words, that it made a good copy, and associated the right file/path information.

Strategic Point--Person Who Collected Data:



The same considerations apply to the technician who collected the data. Even if the tools were correct, if they were used by an untrained person the ESI may be suspect. Counsel must find out if the collection

technician used the tool properly. Counsel should ask about the credentials of the collections staff. Forensic grade collection requires training and experience as well as good tools. A general office worker is unlikely to understand forensic collections. A member of the client's IT staff may not be any more knowledgeable. The technician should have baseline certifications such as EnCe (EnCase Certified Examiner) or ACE (AccessData Certified Examiner). Lacking such certifications, the ESI collector should at least have on the job training such as working in a law enforcement forensics group.

15.17[5] Authenticity of ESI May Be Attacked by Showing Faulty Chain of Custody. Chain of custody documentation must show where a piece of ESI has been at all times, from the time when it resided in its original habitat on the custodian's hard drive, through to its final production version when produced to opposing counsel. Counsel should be able to track a specific piece of ESI offered in court back to its particular origin, and account for any place has been in between. If counsel cannot show the chain of custody, the ESI is vulnerable to evidentiary attack on several levels, starting with authenticity. If the ESI cannot be traced in this manner the jury may not be able to know to know that this ESI is what counsel says it is.

The proponent of the evidence bears the burden of proving appropriate chain of custody. "The burden on the party offering the evidence is to show to the satisfaction of the trial court that, taking all the circumstances into account including the ease or difficulty with which the particular evidence could have been altered, it is reasonably certain that there was no alteration. The requirement of reasonable certainty is not met when some vital link in the chain of possession is not accounted for, because then it is as likely as not that the evidence analyzed was not the evidence originally received. Left to such speculation the court must exclude the evidence. Conversely, when it is the barest speculation that there was tampering, it is proper to admit the evidence and let what doubt remains go to its weight" [*People v. Catlin* (2001) 26 C4th 81, 134, 109 CR2d 31, 26 P3d 357].



Strategic Point--Documenting Chain of Custody.

Chain of custody documentation should start by identifying where the ESI was originally located, and should have a written certification from someone at the original site establishing that site access was provided to the technician who conducted the collection. A log verified by declaration or testimony should list what was collected, where it was collected from, how it was collected, and on what date. From that point on documentation should account for where the ESI was at all times, and what, if anything, was done to it at each site. Good documentation shows each step, from collection, through processing, through load into a review platform, through production. There also may be a need to demonstrate a chain of custody during the time between the time of production and the use of the evidence in trial, particularly when the ESI was produced in native electronic format and had to be printed before its use. If there are gaps, they should be filled in with declarations or testimony. Lacking this information, proffering counsel may not be able to show that the ESI is what counsel says it is. The ESI could be from anywhere, and it may have been improperly processed - altered or tampered with. If there are gaps counsel must find out who knows what happened during the gap.



Cross Reference:

Form for chain of custody declaration, see 15.34.

15.17[6] Evidence of Processing and Manipulation May Be Used to Attack ESI Authenticity. Counsel must seek to understand what, if anything, was done to the data before it was served up as evidence. If anything was done to the ESI which altered its essential nature, it may not be authentic. Counsel should determine whether, after it was collected, anything was done to it to alter or manipulate it. If the ESI is not a straightforward printout of a known data system, counsel should make sure to understand and approve of what was done to create the ESI printout.

Consider:

Not all alterations will defeat authenticity. For example, in order to produce e-mails, e-discovery vendors often strip the e-mail and place its parts in different fields of a review platform--a field for AUTHOR, a field for BCC, a field for the MESSAGE TEXT, etc. In this case, the essential aspects of the e-mail are not really altered, just rearranged to view them and search them better. However, if a database was pulled apart and reassembled, the question is whether it was reassembled properly. If it was not, the data may not be authentic; that is, a true representation of the database as it resided at the parent company. If anything was done to the ESI after collection, counsel should determine whether those processes altered the data in any essential way.



160 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial

III. ESTABLISHING OR ATTACKING THE AUTHENTICITY OF ESI EVIDENCE

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.18

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.18 Expert Assistance Is Essential for Establishing or Attacking ESI Technical Authenticity.

If counsel wishes to make one of the more technical arguments for or against authenticity, counsel should seek and engage an expert on forensic collections. If counsel already engaged such an expert to assist with creating and responding to discovery requests, that person or firm can also assist in establishing or attacking ESI evidentiary showings. Determining whether a database has been altered or manipulated clearly requires a qualified ESI forensic expert.



161 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial

IV. APPLYING THE HEARSAY RULE AND ITS EXCEPTIONS TO ESI

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.19

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.19 CHECKLIST: Applying the Hearsay Rule and Its Exceptions to ESI

☐ Is ESI evidence being offered to show truth of some matter presented by its contents, or for some other purpose?

Authority:

CCP § 1200

Discussion:

See 15.21

☐ Is ESI evidence being offered computer-generated information, as distinguished from computer-stored information?

Authority:

CCP § 1200; *People v. Hawkins* (2002) 98 CA4th 1428, 1449-1450, 121 CR2d 627

Discussion:

See 15.22

☐ Was ESI record created from a system owned/used/relied upon by a "business" as defined in *Evid Code* § 1270?

Authority:

Evid Code § 1270

Discussion:

See 15.25[1],[2]

☐ If ESI is the record of a business, is it being offered to prove occurrence of an act, condition, or event?

Authority:

Evid Code §§ 1270, 1271

Discussion:

See 15.25[1]

☐ If ESI is the record of a business, was it created in regular course of that business?

Authority:

Evid. Code §§ 1270, 1271

Discussion:

See 15.25[4]

☐ If ESI is the record of a business, do sources of information, and method and timing of preparation, indicate trustworthiness of this information?

Authority:

Evid. Code §§ 1270, 1271

Discussion:

See 15.25[5],[6]

☐ If ESI is the record of a business, is an appropriate witness available who can testify to identity of information as a record of the business, and method of its preparation?

Authority:

Evid. Code §§ 1270, 1271

Discussion:

See 15.25[6]-[8]

☐ If ESI is offered as a public record, was it created by and within the scope of duty of a public employee?

Authority:

Evid Code §§ 195, 1270, 1280

Discussion:

See 15.26



162 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
IV. APPLYING THE HEARSAY RULE AND ITS EXCEPTIONS TO ESI

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.20

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.20 Options and Strategy.

Counsel may encounter hearsay issues in connection with admitting ESI into evidence, or wish to raise such issues in attempting to exclude ESI. Certain hearsay exceptions require a special understanding of the nature of the ESI, or a specialized foundational showing, when applied to ESI evidence.

Counsel do not usually have problems with applying hearsay exceptions to ESI such as e-mails or MS PowerPoint documents. These look enough like their paper counterparts that counsel are both comfortable with them and familiar with the ways to apply hearsay rules. It is not difficult to identify a statement in an e-mail as a statement against interest [see *Evid Code* § 1230] or an admission by a party opponent [see *Evid Code* §§ 1220, 1221].

Difficulties arise, however, with complex ESI systems such as financial databases and record storage systems. These are often multi-dimensional and therefore do not print out well. They are usually considered hearsay because someone entered the information into them. Information entered into a database by a person can be a "statement" subject to the hearsay rule.

Example:

A financial database record that party X paid a stated amount on the party's account on date Y. If the record is being offered for the truth of those facts--that X actually did pay that amount on that date--the computer record is hearsay. (Conversely, information *created by the computer* and stored in a database is likely not a "statement" for purposes of the hearsay rule.)

The usual hearsay exemptions applied to complex data systems are:

- The business records exemption [see 15X.25].
- The public records exemption [see 15X.26].
- The "other indicia of trustworthiness" catch all exemption [see 15X.27].

Each of these exemptions presents special issues when applied to ESI systems.

► **Cross Reference:**

General discussion of hearsay evidence issues, see *Matthew Bender(R) Practice Guide: California Trial and Post-Trial Civil Procedure, Ch.11, Questioning Witnesses and Objections, § 11.103.*



163 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial

IV. APPLYING THE HEARSAY RULE AND ITS EXCEPTIONS TO ESI

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.21

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.21 Hearsay Is Defined by Statute.

The Evidence Code defines hearsay as a statement made by someone other than a witness who is testifying at the trial or hearing, which is being offered to prove the truth of the matter stated. The out-of-court "statement" can be oral or written [*Evid Code* §§ 1200(a), 225; see *Brake v Beech Aircraft Corp.* (1986) 184 CA3d 930, 229 CR 336 (computer-generated statistical analysis comparing accident rates for the type of aircraft that crashed with rates for other aircraft on a per flight basis is inadmissible hearsay in a wrongful death action)].



164 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
IV. APPLYING THE HEARSAY RULE AND ITS EXCEPTIONS TO ESI

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.22

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.22 Computer Generated Information May Not Be Hearsay.

California courts distinguish between electronic records which are simply *stored on* a computer (computer-stored information), and information which is *generated* through the use of a computer (computer-generated information). If the information which counsel wishes to offer is computer-generated information, it may not be hearsay at all.

Example--Distinction Between Computer-Stored and Computer-Generated Records:

An employee writes a memo, and stores it on the company server. The ordinary contents of the memo--the user-generated data in the memo that is visible when the memo is printed out--is subject to ordinary hearsay considerations, because a human author made representations in the memo and that author had the usual temptations to lie or misrepresent, or might simply have been ignorant of the true facts. However, the user's computer created metadata and applied it to the document--such as the "create date," the identity of the author, and the date last modified. The computer made this information, not a human being, and it did so through pre-existing programming functions that existed on the computer.

At least one California court has pointed out that computer-generated information such as metadata and system logs should not be considered hearsay at all [*People v. Hawkins* (2002) 98 CA4th 1428, 1449-1450, 121 CR2d 627] . The court held that the hearsay rules were created to overcome problems which pertain to human testimony, and have no application to computer-generated data of this kind. Therefore, the court decided that hearsay rules need not apply to computer generated evidence. Instead, to admit this kind of evidence, all the proponent need show is that the information was computer-generated (rather than human-generated) and that the computer in question was operating properly at the time the information was generated [*People v. Hawkins* (2002) 98 CA4th 1428, 1449-1450, 121 CR2d 627] .

Example--Computer-Generated Information Is Not Hearsay.

In a criminal matter, the defendant was found guilty of the felony offense of knowingly accessing and taking data from a computer system [*Pen Code* § 502(c)(2)]. Part of the defendant's appeal focused on computer printouts from defendant's home system, on which his computer had date-stamped the files. The prosecutor claimed that the printouts showed that the defendant accessed his former employer's source code on dates after he had terminated his employment. The defendant argued that they were inadmissible hearsay and that the prosecutor had failed to establish an applicable hearsay exception. The court distinguished between computer-stored information and computer-generated information, and held

that the latter was not hearsay, and held that the trial court did not abuse its discretion in admitting evidence of the computer printouts, since the trial court based its ruling on the prosecutor's offer of proof that the computer clock was functioning properly [*People v. Hawkins* (2002) 98 CA4th 1428, 1449-1450, 121 CR2d 627] .



165 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
IV. APPLYING THE HEARSAY RULE AND ITS EXCEPTIONS TO ESI

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.23

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.23 Hearsay Is Inadmissible Except As Otherwise Permitted by Law.

15.23[1] General Rule Is That Hearsay Is Inadmissible. The general rule is that hearsay evidence is inadmissible [*Evid Code* § 1200(b)]. Thus, ESI information qualifying as hearsay must come within one of the exceptions to this rule in order to be admissible.

Consider--Rationale for Hearsay Rule:

The rationale for this bar is that when a statement is offered through hearsay evidence, the person who made the statement is not available for cross-examination. In criminal matters, this lack of cross-examination can affect the defendant's constitutional right to confront his or her accusers [*USCS Const. Amend. 6*; *Evid Code* § 1204; *Ohio v. Roberts* (1979) 448 US 56 , 100 SCt 2531, 65 LEd2d 597 (*Confrontation Clause* does not require blanket exclusion of hearsay evidence); *People v. Kons* (2003) 108 CA4th 514, 133 CR2d 520 (hearsay evidence was properly admitted and did not deny appellant his constitutional right to confront accusers)].

In civil matters, the primary judicial policy objection to hearsay evidence is that the declarant is not being made subject to cross-examination. Without cross examination, the reliability or trustworthiness of the witness and their statement cannot be adequately tested [*see Brake v Beech Aircraft Corp.* (1986) 184 CA3d 930, 229 CR 336 (computer-generated statistical analysis comparing accident rates for type of aircraft that crashed with rates for other aircraft on a per-flight basis is inadmissible hearsay in wrongful death action)].

15.23[2] Hearsay Is Admissible If Sufficiently Trustworthy. Even if a statement is made outside of court, and the witness is not made available for cross-examination, the item being offered may have other qualities which indicate that it is trustworthy and can be relied upon. The goal of the hearsay exceptions is to identify what kinds of hearsay are inherently trustworthy and reliable [*Evid Code* § 125 (hearsay is inadmissible if the statement was made under circumstances that indicate its lack of trustworthiness); *In re Cindy L.* (1997) 17 C4th 15, 27-28, 69 CR2d 803, 947 P2d 1340 ; *People v Kons* (2003) 108 CA4th 514, 133 CR2d 520 (hearsay evidence was properly admitted and did not deny appellant his constitutional right to confront accusers)].



166 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
IV. APPLYING THE HEARSAY RULE AND ITS EXCEPTIONS TO ESI

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.24

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant**15.24 Hearsay Is Admissible If It Falls Within an Exception to General Rule.**

15.24[1] California Statutes Provide Numerous Hearsay Exceptions. The California codes state many accepted exceptions to the hearsay rule [see, e.g., *Evid Code* §§ 1200-1380; *People v. Spriggs* (1964) 60 C2d 868, 36 CR 841, 389 P2d 377 (hearsay exception codified in *Evid Code* § 1230); *Nardoni v. McConnell* (1957) 48 C2d 500, 310 P2d 644 (statutory exception contained in *Gov Code* § 11513(c)); *In re Michael V.* (1986) 178 CA3d 159, 223 CR 503 (statutory exception contained in *W&I Code* §§ 706, 725.5)]. These statutory hearsay exceptions are intended to provide a safe harbor when the trustworthiness of particular types of records has been sufficiently litigated that courts are comfortable with offering a blanket ruling that this kind of record is trustworthy. Evidence that falls within a particular exemption is deemed trustworthy and therefore is not barred because it is hearsay.

15.24[2] Nonstatutory "Catch All" Hearsay Exception Exists for "Other Indicia of Trustworthiness." The California Evidence Code does not contain a specific "residual" hearsay exception such as that enumerated in *Fed. Rules of Evidence*, Rule 807. However, the California Supreme Court has affirmed that the statutory hearsay exceptions are not intended to define the only available exceptions. Hearsay exceptions are not limited to those enumerated in the Evidence Code, and "may also be found in other codes and decisional law" [*In re Malinda S.* (1990) 51 C3d 368, 376, 272 CR 787, 795 P2d 1244] .

**Strategic Point:**

The gate for admission of hearsay evidence has been left open, but not unguarded. The challenge for counsel is to find and present facts which pertain to the reliability of the record being offered. Counsel must show sufficient indicia of trustworthiness that a court can conclude that the statements are likely to be accurate [see *In re Cindy L.* (1997) 17 C4th 15, 27-28, 69 CR2d 803, 947 P2d 1340] .



167 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial

IV. APPLYING THE HEARSAY RULE AND ITS EXCEPTIONS TO ESI

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.25

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.25 ESI May Be Admissible Under Business Records Exception to the Hearsay Rule.

15.25[1] Business Records Are Admissible Hearsay. Under the business records exception to the hearsay rule, if the ESI is being offered to show the occurrence of an act, condition, or event recorded there, it is admissible despite the hearsay if all of the following are true [*Evid Code* § 1271]:

- The ESI was created "in the regular course of business";
- The ESI was created at or near the time of the act, condition or event;
- A custodian or other qualified witness testifies as to the identity of the ESI as a record of the business, and as to the mode of its preparation; and
- The sources of information used to create the record, and the method and timing of its preparation, all indicate that it is trustworthy.

The exception pertains to records that were made without a litigation motive, and which the business created in order to rely upon it in the conduct of its day-to-day business affairs. Further, the exception is limited to those records with respect to which the proponent can show that the business put some effort into quality control; in other words, that it had some kind of process for the creation of the record which supports the assumption that the record is accurate [*Evid Code*, § 1271 (commentary); *People v. Crosslin* (1967) 251 CA2d 968, 60 CR 309 (fingerprint card); *People v. Gorgol* (1953) 122 CA2d 281, 265 P2d 69 (fact that they are hearsay does not preclude admission)].

Consider--Purpose of the Business Records Exception.

As with all hearsay exceptions, the business records exception exists to serve judicial economy. Courts have long recognized that records made and relied upon in the regular course of business are likely to be trustworthy, and that a lengthy verification process by all persons who contribute to them does not add much to judicial safeguards.

15.25[2] Statutory Definition of "Business" Includes Governments and Nonprofits. The definition of a

"business" under *Evid Code* § 1270 includes both "governmental activity" and "operation of institutions, whether carried on for profit or not." Therefore, if government records, or the records of a non-profit meet the other requirements of the business records exception to the hearsay rule, they can be admitted into evidence as "business records" [*Evid Code* § 1270 and Law Revision Commission Commentary].

15.25[3] Court Has Discretion Regarding Qualification As Business Record. California courts have great discretion in determining whether or not the proponent has laid a sufficient foundation to qualify an item as a business record. The court's decisions on this point will be overturned only on a clear showing of abuse of discretion [*County of Sonoma v. Grant W.* (1986) 187 CA3d 1439, 1450-1451, 232 CR 471 ; *Trans-World Airlines, Inc. v. Alitalia-Linee Aeree Airlines* (1978) 85 CA3d 185, 192, 149 CR 411] .

15.25[4] ESI Must Have Been Prepared in the "Ordinary Course of Business." The first requirement for the business records exception is that the ESI *must have been created in the ordinary course of business* [*Evid Code* § 1271(a)]. The reasoning behind this requirement is the idea that if the intent was to create a business record that would be used to support ordinary business activities, the business had no real motive to fabricate or skew the record. The business needed the record to be accurate so that it would be usable.

Therefore, counsel wishing to proffer or attack a piece of ESI must examine the reasons for the creation of the record and the manner in which it was created, and ask the following questions:

- Was the record created by a reliable employee or other agent of the business to support regular business activities?
- What activities?

Example--Record Not Created "In the Ordinary Course of Business":

Driver A filed an SR1 form with the DMV reporting an alleged automobile accident, as required by law. When Driver B did not file an SR1, the DMV suspended Driver B's driver's license. Driver B demanded a formal hearing. The only evidence offered regarding the occurrence of the alleged accident was the SR1 filed by Driver A. The court noted that it was the regular duty of the DMV to receive such reports and to keep them. However, it was not the ordinary course of business for the citizen author to make such a report to the DMV. The court held that the SR1 was inadmissible hearsay because the report made by Driver A was not made "in the ordinary course of business" [*Daniels v. DMV* (1981) 33 C3d 532, 537-538 ; 189 CR 512, 658 P.2d 1313] .

It may also be important to take in to consideration the nature of the business. For example, if the business is in the business of creating litigation support materials, the ESI may still be inadmissible even though it is the kind of record the business makes during an ordinary business day. Litigation gives different motives than the orderly running of day to day business process [*Evid Code* § 1271(a); see *People v. Hernandez* (1997) 55 CA4th 225, 241, 63 CR 2d 769 (records in police database of investigative reports were not admissible under business record exception); *Melendez-Diaz v. Massachusetts* (2009) ___ US ___, 129 S Ct 2527, 2538, 174 L Ed2d 314 (lab reports prepared for police were not admissible business record under Fed R Evid 803(6)); *Palmer v. Hoffman* (1943) 318 US 109, 63 S Ct 477, 87 L Ed 645 (statement given to railroad investigators following train accident was not within scope of a regular business activity)].

15.25[5] ESI Must Have Been Created at or Near the Timing of Act, Condition, or Event. The second requirement of the business records exception is that the ESI record *must have been created at or near in time to the occurrence of the act, condition or event* [*Evid Code* § 1271(b)]. This requirement is fairly fluid, and what constitutes "near" is in the sound discretion of the deciding court [see, e.g., *Molenda v. DMV* (2009) 172 CA4th 974 ; 91 CR3d 792 (computerized lab report created 8 days after performance of blood alcohol content test was not created "near" the occurrence of the act or event as required by hearsay exception); but see *Komizu v. Gourley* (2002), 103 CA4th 1001,

127 CR2d 229 (report of appellant's blood alcohol content, typed six days after appellant's blood was analyzed, was properly admitted into evidence as it was recorded on or near the event for purposes of public employee record exception under *Evid Code* § 1280)).

Consider--Operative Date Is Date of Data Entry, Not Date of Printout.

With regard to ESI evidence, the key consideration is the timing of the data entries that make up the record. The "business record" is not necessarily the printout that counsel is holding in his or her hands. The "business record" is the underlying data system that was used to create that report, and the relevant date therefore is the date on which the data was entered into the system. If the data was not entered or otherwise created "at or near" the events it records, the "business record" does not meet the requirements of the hearsay exception [*Aguimatang v. California State Lottery* (1991) 234 CA3d 769, 286 CR 57 (date of challenged computer printout was immaterial; challenged data was entered onto computer system contemporaneously with events recorded and therefore printouts qualified as business records)].

15.25[6] Custodian Must Testify Regarding Identity and Methods of Preparation. The business records exception requires that the proponent provide testimony from a "qualified witness" who can provide testimony regarding the fact that the record is indeed a record of the particular business, and regarding the methodology employed by the business to prepare it [*Evid Code* § 1271(c)].



Strategic Point:

The requirements to be a qualified witness are not onerous. The witness need not be a computer or business process expert. The witness need only be familiar with the procedures followed to create the record, and be able to describe them. The witness need not have been personally involved in the data entry or preparation of the particular business record in order to be "qualified." Neither must the witness be the regular custodian of the record [*Jazayeri v. Mao* (2009) 174 CA4th 301, 324, 94 CR3d 198 (reversing exclusion of business records); *People v. Hovarter* (2008) 44 C4th 983, 1012, 81 CR3d 299, 189 P3d 300] .

Example--Incorrect Custodian Offered.

In a case of theft by misappropriation, a check from the records of a title company was offered to show that the title company had suffered a loss of \$78,000. The problem was that the original title company involved in the transaction had been taken over by another company. The custodian who testified concerning the records was an officer of the successor company, and could not provide testimony regarding the former company's methods and procedures. This testimony was not sufficient to support admission of the evidence under the business records exception to the hearsay rule [*People v. Shirley* (1978) 78 CA3d 424 ; 144 CR 282] .

15.25[7] Custodian Need Not Testify That Computer Is Reliable. California law differentiates between the system or series of steps used to create a record, and the computers used to mechanize that system. A witness attempting to qualify a computer record as a business record needs to provide information regarding the system used to create the record--the string of steps and methods used to create the record. This establishes that the record was created using regular practices and procedures, as required by the business records exception to the hearsay rule [*People v. Lugashi* (1988) 205 CA3d 632, 640, 252 CR 434] .

Stated another way, there is no presumption that computers are unreliable [*People v. Lugashi* (1988) 205 CA3d 632, 642, 252 CR 434] . Usually, the reverse is true--a business tries to use computers and software that function properly, and that are designed to provide accurate results. Therefore, as long as the methods to create the data are explained, the burden of proof then shifts to the opponent to show that the steps described, or the particular computers, are somehow unreliable. Without such a showing, the ESI evidence is admissible [see *Santos v. Department of Motor Vehicles*

(1992) 5 CA4th 537, 7 CR2d 10 (absent evidence that report was not properly prepared, DMV was entitled to rely on it)].

The custodian is not required to opine on the subject of the reliability of the business process used to create the data, or that the computers used to process or store the data were reliable, or that the software used to process the data uses methodology which is acceptable in the scientific community. The custodian need not be an expert [*People v. Lugashi* (1988) 205 CA3d 632, 642, 252 CR 434, 440] .



Strategic Point--Proponent:

If the proper functioning of the computers themselves is appropriately challenged, the proponent of the ESI should be prepared to produce a witness to testify that the computer was operating properly [*People v. Hawkins* (2002) 98 CA4th 1428, 1450, 121 CR2d 627] .

15.25[8] Testimony Must Show Trustworthiness. The sources of information and method and time of preparation must be such as to indicate the trustworthiness of the ESI [*Evid Code* § 1271(d)]. Therefore, although the custodian is not required to be an expert, the custodian's testimony, or that of others, nevertheless should support a finding that the methodology used was reasonable under the circumstances, and that the resulting record is reliable and trustworthy. The following questions should be addressed in this regard:

- How is the data selected for input into the computer system?
- How does one know that this source is reliable?
- If there are other possible sources for this information, why was this one selected?
- Are there quality controls to ensure that data entry is accurate and properly represents the information in the source item?
- Does the business rely upon these records?
- Have the records been shown to be reliable over time?
- Have the records been shown to be unreliable over time (for example, have there been customer or government complaints)?

The answers to these kinds of questions can be presented in the custodian's testimony, providing facts on which the court may exercise its discretion and admit the ESI into evidence. The court's decisions on this point will be overturned only upon a clear showing of abuse of discretion. [*County of Sonoma v. Grant W.* (1986) 187 CA3d 1439, 1450-1451, 232 CR 471 ; *Trans-World Airlines, Inc. v. Alitalia-Linee Aeree Airlines* (1978) 85 CA3d 185, 192, 149 CR 411] .



168 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial

IV. APPLYING THE HEARSAY RULE AND ITS EXCEPTIONS TO ESI

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.26

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.26 ESI May Be Admissible Under the Official Records Exception to the Hearsay Rule.

15.26[1] Official Records Exception Applies to Records Made by Public Employees. ESI may be admissible under the official records exception to the hearsay rule. Under the official records exemption, a writing made as a record of an act, condition, or event is admissible to prove the occurrence of the act, condition or event if all of the following conditions are satisfied [*Evid Code* § 1280]:

- The writing was made by and within the scope of duty of a public employee [*see* 15.26[2];
- The writing was made at or near the time of the act, condition, or event [*see* 15.26[3]]; and
- The sources of information and method and time of preparation were such as to indicate its trustworthiness event [*see* 15.26[4]].

15.26[2] ESI Must Have Been Prepared by a Public Employee Acting Within the Scope of Duty.

15.26[2][a] "Public Employee" Is Broadly Defined. "Public employee" is defined as an officer, agent, or employee of a public entity [*Evid Code* § 195]. The section is intentionally broad and covers more than a typical person who is directly employed as a civil servant in a public agency.

15.26[2][b] Public Employee Must Create Rather Than Simply Accept or Store Data. If an agency only receives and houses the data, but did not create it, it was not prepared by a public employee acting within the scope of duty as required by *Evid Code* § 1280(a). Thus, counsel must show who actually created the original data.

Example:

The California Supreme Court upheld a trial court's decision to exclude a DMV Form SR1 accident report, holding that because the SR1 was prepared by a driver, it was not admissible under the official records exclusion. It did not matter to the court that it was the regular practice of the DMV to require, accept, and store such reports. Since a DMV employee did not prepare it, it was not an official record within the meaning of that term in *Evid Code* § 1280 [*Daniels v. DMV* (1981) 33 C 3d 532, 537-538 ;

189 CR 512, 658 P.2d 1313] .

15.26[2][c] ESI Must Be Within Mandate of Agency's or Employee's Duties. If the data was created by public employee, the creation of that data still must be the subject of an official duty [*Evid Code* § 1280(a)]. This involves examination of the following questions [*see Vallejo & N. R. Co. v. Reed Orchard Co. (1915) 169 Cal. 545, 571, 147 P 238* (statistical report of state agency admitted; court judicially noticed the statutory duty to prepare the report)]:

- What is the mandate of the agency that collected the data?
- Is the ESI part of the statutory authority or duties of the agency?
- Does the agency need the information to perform its work?
- Is it required by law to create the data?

Example--Information Not Prepared by Public Employee Within Scope of Duties.

In an airplane crash case, the jury found for the defendant plane manufacturer on statute of limitation grounds. Among the items addressed in the appellate briefs was a General Accounting Office report which the trial court had deemed inadmissible. The report was authored by an unidentified employee of the GAO and allegedly showed that the defendant aircraft manufacturer and other aircraft manufacturers had failed to carry out their responsibilities in connection with the certification process. The court upheld both the jury verdict and the trial court's decision to exclude the report. The appeals court pointed out that not only was the report irrelevant to the matters at hand, the plaintiffs had failed to offer any information as to "the identity and qualifications of the individuals who prepared said report, the facts upon which they based the report, or the circumstances under which it was prepared." In addition, the report was prepared by the GAO, not by any agency that had statutory duties regarding regulation or investigation of airplane safety. The report was not an admissible official report and the trial court properly refused to take judicial notice of it [*Baker v. Beech Aircraft Corp. (1979) 96 CA3d 321, 338, 157 CR 779* ; *see Elsworth v. Beech Aircraft Corp (1984) 37 C3d 540, 208 CR 874, 691 P2d 630* (discussing and also excluding the same GAO report)].

15.26[3] ESI Must Have Been Made at or Near the Time of Act, Condition, or Event. The ESI in question must have been made "at or near" the time of the act, condition or event recorded [*Evid Code* § 1280(b)]. This requirement is fairly fluid, and what constitutes "near" is in the sound discretion of the deciding court [*see, e.g., Molenda v. DMV (2009) 172 CA4th 974* ; *91 CR3d 792* (computerized lab report created eight days after performance of blood alcohol content test was not created "near" the occurrence of the act or event as required by hearsay exception); *but see Komizu v. Gourley (2002), 103 CA4th 1001, 127 CR2d 229* (report of appellant's blood alcohol content typed six days after appellant's blood was analyzed, was properly admitted into evidence as it was recorded on or near the event as required by *Evid Code* § 1280)].

Consider--Operative Date Is Date of Data Entry, Not Date of Printout.

As with business records in ESI format, counsel must not focus on the printout. Since a printout is nothing more than a means of communicating data, the timing requirement does not pertain to the date when the printout was made. The critical issue is the date when the data entries which make up the printout were originally made [*Lee v. Valverde (2009) 178 CA4th 1069, 100 CR3d 867*] .

Example--ESI Entry Not Made "At or Near" Time of Occurrence.

The defendant was stopped by a police officer who arrested him for DUI and arranged for taking a blood sample. The DMV held a hearing and suspended his driver's license. The evidence at issue was a lab report which allegedly showed the defendant's blood alcohol content and was the sole evidence of blood alcohol level offered at the administrative hearing. It was entered into the DMV's computer database

eight days after the blood sample had been taken from the defendant. At the hearing, the defendant objected to the report as hearsay. The hearing officer apparently relied upon it anyway. When the driver appealed to a trial court, the DMV argued that the report was admissible as an official record. The trial court refused to admit the report, reasoning that the official records exemption requires that the record in question be made near in time to the occurrence it purports to prove. The court held that the time lapse was too long to meet the "near in time" requirement [*Molenda v. DMV* (2009) 172 CA4th 974, 91 CR3d 792] .

Example--ESI Entry Was Made "At or Near" Time of Occurrence.

The defendant driver was stopped for DUI and his license was suspended after an administrative hearing. He appealed, and the trial court ruled in his favor, holding that the forensic report establishing that the driver was driving with a blood alcohol concentration of 0.08 percent or higher had been improperly admitted at the administrative hearing. The appellate court overturned, on the grounds that the trial court had abused its discretion. The appeals court reasoned that the forensic report was nothing more than a computer printout of the results of the blood test, which was both analyzed and reported on May 30, 2007. Thus, the June 19, 2007, date on the report was simply the date it was printed or "published," not the date the test was reported. Hence, the report was admissible under the public records exception to the hearsay rule because the report was made on the same date the test was conducted. The fact that the test results were re-reported or subsequently "published" did not cause any danger of inaccuracy by lapse of memory [*Lee v. Valverde* (2009) 178 CA4th 1069, 100 CR3d 867] .

15.26[4] Sources, Methodology, and Timing Must Indicate Trustworthiness.

15.26[4][a] Trustworthiness Must Be Shown. The official records exception, like the business records exception, requires a showing that the sources of information and method and time of preparation were such as to indicate its trustworthiness [*Evid Code* § 1280; see 15.25[8]].

15.26[4][b] Trustworthiness May Be Proved Without Witness Testimony. Unlike the business records exception, the official records exception does not require that the proffering party produce a witness to identify the records, or to describe the mode of preparation [*compare Evid Code* §§ 1271, 1280; see 15.25[6] (business records exception)]. The Law Revision Commission comments to *Evid Code* § 1280 specifically state that the Commission's intent was not to require that proffering parties prove identity and mode of preparation through witness testimony. Under *Evid Code* § 1280, the proffering party is free to make this showing other ways. The showing still must be made; it simply need not be accomplished using witness testimony. Whether the trustworthiness requirement has been met is a matter within the trial court's discretion [*People v. Dunlap* (1993) 18 Cal. App. 4th 1468, 23 Cal. Rptr. 2d 204, cert. denied, (1994) 511 US 1087] .

Assuming satisfaction of the exception's other requirements, the trustworthiness requirement may be established by a showing that the written report is based upon the observations of public employees who have a duty to observe the facts and report and record them correctly [*Gananian v. Zolin* (1995) 33 CA4th 634, 39 CR2d 384] .

15.26[4][c] Trustworthiness May Be Proved by Judicial Notice. Proof by judicial notice is one of the additional methods contemplated by the Law Revision Commission [*Evid Code* § 1280, 1965 Law Revision Commission Comments; see *People v. Williams* (1883) 64 C 87, 27 P 939 (census report admitted; court took judicial notice of statutes prescribing method for preparing report); *Vallejo & N. R. Co. v. Reed Orchard Co.* (1915) 169 C 545, 571, 147 P 238] .

The following matters *must* be granted judicial notice in California [*Evid Code* § 451]:

- The decisional, constitutional, and public statutory law of California and of the United States, and the provisions of any charter described in *Cal Const Art. XI*, §§ 3, 4, or 5.

- Any matter made a subject of judicial notice by *Gov Code* §§ 11343.6, 11344.6, or 18576 or 44 USC § 1507.
- Rules of professional conduct for members of the bar adopted pursuant to *Bus & Prof C* § 6076, and rules of practice and procedure for California courts adopted by the Judicial Council.
- Rules of pleading, practice, and procedure prescribed by the United States Supreme Court, such as the Rules of the United States Supreme Court, the Federal Rules of Civil Procedure, the Federal Rules of Criminal Procedure, the Admiralty Rules, the Rules of the Court of Claims, the Rules of the Customs Court, and the General Orders and Forms in Bankruptcy.
- The true signification of all English words and phrases and of all legal expressions.
- Facts and propositions of generalized knowledge that are so universally known that they cannot reasonably be the subject of dispute.

The following matters *may* be granted judicial notice in California [*Evid Code* § 452]:

- The decisional, constitutional, and statutory law of any state of the United States and the resolutions and private acts of the Congress of the United States and of the California Legislature.
- Regulations and legislative enactments issued by or under the authority of the United States or any public entity in the United States.
- Official acts of the legislative, executive, and judicial departments of the United States and of any state of the United States.
- Records of any California court, or any court of record of the United States or any state of the United States.
- Rules of court of any California court, or any court of record of the United States or any state of the United States.
- The law of an organization of nations and of foreign nations and public entities in foreign nations.
- Facts and propositions that are of such common knowledge within the territorial jurisdiction of the court that they cannot reasonably be the subject of dispute.
- Facts and propositions that are not reasonably subject to dispute and are capable of immediate and accurate determination by resort to sources of reasonably indisputable accuracy.



Cross Reference:

For a more general discussion of judicial notice and admissibility, see Cotchett, California Courtroom Evidence, Ch. 12, Judicial Notice Evidence.

Example--Judicial Notice That Record Was Timely Made.

In a criminal prosecution, a computer printout of appellant's criminal information history ("rap sheet") was admitted under the official records exception to the hearsay rule for the purpose of showing that the defendant had served two prior prison terms, thereby enhancing his sentence. The appellate court held

that the trial court properly admitted the rap sheet. The official records exception to the hearsay rule did not require that the prosecutor offer testimony by a custodian or other qualified witness as to the identity and mode of preparation of the record. Instead, *Evid Code* § 664 authorized the trial court to take judicial notice of statutes requiring Department of Justice personnel to record the information on the rap sheet within a short period of its receipt from the reporting agency, thereby meeting one of the foundational requirements for admissibility. Further, the trial court had discretion to determine whether the foundational requirement of trustworthiness was met [*People v. Dunlap* (1993) 18 CA4th 1468, 23 CR2d 204 , cert. denied, (1994) 511 US 1087] .

15.26[4][d] Proffering Party May Invoke Presumption That an Official Duty Was Regularly Performed.

When the law requires that a public employee or agent of a public agency perform a duty, such as collection and recording of data, *Evid Code* § 664 establishes a statutory presumption that this duty was regularly performed. The court may take judicial notice of the duty and no further evidence is required [*Evid Code* § 664; *Bhatt v. State Dept. of Health Services* (2005) 133 CA4th 923, 35 CR3d 335 (printouts of Medi-Cal records were admissible under hearsay exception for official records because statute presumes the official duties shown were regularly performed and plaintiff offered no evidence to rebut this presumption)]. One way that the party proffering evidence can avoid offering a witness to testify regarding the methodology used to prepare an ESI record is to rely on this presumption.

This presumption acts to shift the burden of proof. The proffering party does not need to prove the record was created properly. The party attempting to suppress the evidence must show instead that the record was not made properly; in other words, that the employee or agency did not have a statutory duty to perform the act or record the data, or that something untoward happened in the preparation of this particular record. The objecting party must prove that the presumed fact did not happen [*People v. Martinez* (2000) 22 C4th 106, 91 CR2d 687, 990 P2d 563] .

Example--Presumption That Statutory Duties Were Properly Performed.

At a Department of Motor Vehicles administrative hearing on the suspension of a driver's license for driving while intoxicated, the result of the laboratory test of the driver's blood was properly admitted under the public employee records exception to the hearsay rule [*Evid Code* § 1280], even though it did not indicate the time it was prepared so as to demonstrate that it was made "at or near the time of the act, condition, or event" as required by *Evid Code* § 1280(b). The presumption of duty regularly performed [*Evid Code* § 664] shifted the burden to the driver to show that the report was not properly prepared. In the absence of evidence that the report was not properly prepared, the department was entitled to rely upon it [*Santos v. Department of Motor Vehicles* (1992) 5 CA4th 537, 7 CR2d 10] .

Example--Statutory Presumption Inapplicable to ESI in Question.

The defendant was stopped by a police officer who arrested him for DUI and arranged for taking of a blood sample. The DMV held a hearing and suspended his driver's license. The evidence at issue was a lab report that allegedly showed the defendant's blood alcohol content. The lab report was the sole evidence of blood alcohol level offered at the administrative hearing. It was entered into the DMV's computer database eight days after the blood sample had been taken from the defendant. At the hearing, the defendant objected to the report as hearsay, but the hearing officer apparently relied upon it anyway. When the driver appealed to a trial court, the DMV argued that the report was admissible as an official record. The trial court refused to admit the report, reasoning that the official records exemption requires that the record in question be made near in time to the occurrence it purports to prove. The court held that the time lapse was too long to meet the "near in time" requirement. Furthermore, the court refused the DMV's request that the court presume that the test results were timely recorded under *Evid Code* § 664, the presumption that an official duty has been regularly performed, because no statute or regulation imposed a timeliness duty upon the DMV or its agents with regard to the recording of the test results [*Molenda v. DMV* (2009) 172 CA4th 974, 91 CR3d 792] .



169 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
IV. APPLYING THE HEARSAY RULE AND ITS EXCEPTIONS TO ESI

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.27

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.27 ESI May Be Admissible Under Catch All Hearsay Exception by Showing Other Indicia of Trustworthiness.

The statutory hearsay exceptions are not intended to define the only ways to admit hearsay evidence [*In re Malinda S. (1990) 51 C3d 368, 376, 272 CR 787, 790, 795 P2d 1244, 1274* (exceptions to hearsay rule are not limited to those enumerated in Evidence Code, and also may be found in other codes and decisional law); *see 15.23[2]*]. If counsel is unable to fit the ESI into one of the specific statutory exceptions, it may be possible to invoke a less structured exception.

To get hearsay admitted on this basis, counsel must show sufficient indicia of trustworthiness that a court can conclude that the statements are likely to be accurate [*see In re Cindy L. (1997) 17 C4th 15, 27-28, 69 CR2d 803, 947 P2d 1340*]. Counsel needs to come up with a plan that assures the court that the information is trustworthy. Whether the trustworthiness requirement has been met is a matter within the trial court's discretion [*People v. Dunlap (1993) 18 CA4th 1468, 23 CR2d 204, cert. denied, (1994) 511 US 1087*].



Strategic Points--Demonstrating That ESI Source Is Trustworthy.

In presenting evidence that proffered ESI is trustworthy, counsel should consider presenting information on the following points:

- How were the system inputs selected--was the data selected from a reliable source? This is what *Evid Code* §§ 1271 and 1280 are aiming for with the requirement that ESI entries must be made at or near the time of the events they purport to record. Timing is one way to show reliability. There are others. What makes the data in this system reliable (or unreliable)?
- If someone selected the data, what were the credentials and motives of the person(s) who created the data file [*see Daniels v. DMV (1981) 33 C 3d 532, 537-538; 189 CR 512, 658 P.2d 1313* (accident report filed by a driver involved in alleged accident was not necessarily a reliable source of information regarding accident)]?
- How will someone else be able to know that the data is accurate as entered? This is the kind of

testimony which is often introduced to defend business records. How do we know the data in the system is accurate? Were there quality controls on the data entry? Did anyone check the system entries against the source items? Were figures independently added up to see if the totals matched the totals from the originals [see *Evid Code* §§ 1271(d), 1280(c)]?

- If the ESI was processed in a non-straightforward manner, the process will need to be explained and defended. For example, if all the storage program did was add up columns of figures, as in a spreadsheet, that is fairly straightforward. If a special program or algorithm was written and applied to the data set, it will need to be explained. Did the program use industry standard processes, or were they experimental and untested? Was the methodology generally accepted in the relevant scientific community?

- Does anyone rely upon this data file for business purposes or other non-litigation oriented purposes?



170 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
V. APPLYING THE SECONDARY EVIDENCE RULE TO ESI

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.28

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.28 CHECKLIST: Applying the Secondary Evidence Rule to ESI

☐ Is counsel required to present the original to prove its content?

Authority:

Evid Code §§ 1520, 1521(a)

Discussion:

15.30[1],[2]

☐ Does a genuine dispute exist concerning material terms of ESI, such that justice would require exclusion of secondary evidence?

Authority:

Evid Code § 1521(a)(2)

Discussion:

15.30[2]

☐ Is there a likelihood that admission of secondary evidence would be ruled unfair under the circumstances?

Authority:

Evid Code § 1521(a)(2)

Discussion:

15.30[2]

☐ In a criminal action, is original ESI in proponents possession, custody, or control, and has proponent failed to make original reasonably available for inspection at or before trial?

Authority:

Evid Code § 1522(a)

Discussion:

15.30[2]

☐ Is ESI a type that is specifically admissible in criminal proceeding even if proponent has failed to make original reasonably available?

Authority:

Evid Code § 1522(a)(1)-(4)

Discussion:

15.30[2]

☐ Is ESI a printed representation or computer information, a computer program, or images stored in video or digital medium?

Authority:

Evid Code §§ 1552, 1553

Discussion:

See 15.30[3],[4]

☐ Is distinction between original and secondary evidence relevant in this case?

Authority:

Evid Code §§ 255, 260, 1521

Discussion:

15.29, 15.30[1],[2]

☐ If distinction is relevant, and secondary evidence is being presented, was information presented in forensically sound manner.

☐ Is forensically sound source information available for the individual piece of ESI?

Discussion:

15.31

☐ Can oral testimony be used to prove content of ESI?

Authority:

Evid Code § 1523.

Discussion:

15.32



171 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
V. APPLYING THE SECONDARY EVIDENCE RULE TO ESI

*1-15 MB Practice Guide: CA E-Discovery and Evidence 15.29***AUTHOR:** Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant**15.29 Options and Strategy.**

The "secondary evidence rule," California's successor to the traditional "best evidence rule," provides that unless certain conditions exist, the content of a writing may be proved either by introduction of the original writing, or through the use of otherwise admissible secondary evidence [*Evid Code* §§ 1520, 1521; *see former Evid Code 1500* (best evidence rule, *repealed* eff. 1/1/99)]. A party seeking to admit ESI evidence must ensure that the evidence in question is admissible under these criteria. This involves applying such physical-world concepts as "original," "duplicate" and "copy" apply to virtual evidence which may never have had physical presence in a bricks and mortar world.

Consider:

Historically, the best evidence rule enforced a judicial preference for referring to original documents when arguing about the contents [*see, e.g., People v. Wohlleben* (1968) 261 CA2d 461, 67 CR 826 ; *People v. Sloss* (1973) 34 CA3d 74, 109 CR 583] . In 1999, California replaced the best evidence rule with a "secondary evidence rule" allowing proof of a writing by otherwise admissible secondary evidence [*Evid Code* § 1521; Stats. 1998, ch 100 (repealing best evidence rule effective 1/1/1999)].

**Strategic Point:**

Under the secondary evidence rule, otherwise admissible secondary evidence generally is acceptable to the same extent as an original [*Evid Code* § 1521 (a)]. Under some circumstances, however, an original is still required [*see Evid Code* §§ 1521(a)(1),(2), 1522(a), 1532 and discussion in 15.30[2]].

**Cross References:**

For further discussion of the rules and procedures regarding California's secondary evidence rule, *see* California Trial Guide, Unit 31, Secondary Evidence of Writings (Matthew Bender); Imwinkelried & Leach, California Evidentiary Foundations (4th ed 2009), Ch. 7, Secondary Evidence Rule (LexisNexis); Cotchett, California Courtroom Evidence, Ch. 23, Secondary Evidence--Evidence Code §§ 1500-1567.



172 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
V. APPLYING THE SECONDARY EVIDENCE RULE TO ESI

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.30

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.30 Content of Writing May Be Proved by Otherwise Admissible Original.

15.30[1] Content of Writing May Be Proved by Original in All Cases. The content of a writing may be proved by an otherwise admissible original [*Evid Code § 1520*].

15.30[2] Content of Writing *Must* Still Be Proved by Original in Some Cases. If the court is required to exclude secondary evidence, the original is the only option for proving the content of a writing. Thus, even under the liberalized secondary evidence rule, the original can be required by law or statute. For example, the original writing is specifically required in the following circumstances:

- A genuine dispute exists concerning material terms of the writing and justice requires the exclusion [*Evid Code § 1521(a)(1)*].
- Admission of the secondary evidence would be unfair [*Evid Code § 1521(a)(2)*].
- In a criminal action, the court determines that the original is in the proponent's possession, custody, or control, and the proponent has not made the original reasonably available for inspection at or before trial, unless the writing is a "duplicate" [*see Evid Code § 260* (definition) and discussion in 15.31[2]], a writing that is not closely related to the controlling issues in the action, a copy of a writing in the custody of a public entity, or a copy of a writing that is recorded in the public records [*Evid Code § 1522(a)*].

15.30[3] Computer Printout or Other Similar Output Qualifies As an "Original." "Original" means the writing itself or any counterpart intended to have the same effect by a person executing or issuing it. If data is stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original" [*Evid Code § 255; Aguimatang v. California State Lottery (3rd Dist. 1991) 234 CA3d 769, 286 CR 57* (computer printout qualifies as "original")].

Compare:

In contrast a "duplicate" is defined as "a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by

mechanical or electronic rerecording, or by chemical reproduction, or by other equivalent technique which accurately reproduces the original" [*Evid Code* § 260].

When particular ESI has been printed out and exists outside of the computer system, it is easy to categorize the printout itself as an original, and any photocopies made of that original as duplicates [*see Evid Code* §§ 255, 260]. Similarly, if all that is required is to push a button and print out a new copy of the ESI from an electronically-stored copy, the printout would be an original [*see Evid Code* § 255]. Similarly, a copy of the original printout electronically stored in .pdf form, and printed out from that source, arguably would also constitute an original record [*see Evid Code* § 255].

A closer question is presented if the original was created by applying a computer process, or using a specialized program--for example, financial reports generated and printed from a database for a specific meeting--and it is necessary to duplicate the steps or re-run the program in order to re-create the report. The resulting report arguably would be a duplicate, since it is not the first report, even if the underlying data used to generate the new report is unaltered [*see Evid Code* § 260]. However, such a duplicate printout may be indistinguishable from the original. A duplicate could also be created by photocopying the original printout.

Strategic Point:



If the distinction between an original and duplicate is important to counsel's case, new printouts of ESI should be carefully scrutinized to make sure that counsel understands how they were created and how they ought to be characterized.

15.30[4] Computer Printout Is Presumed to Accurately Reflect System Data. A computer printout is entitled to a presumption of accuracy; that is, that it accurately reflects the data contained in the system it printout out from [*Evid Code* § 1552].



Warning:

Evid Code § 1552 does not establish anything other than the fact that a computer's print function has worked properly. The presumption does not establish the accuracy or reliability of the information that is printed out. If the accuracy of the information stored in the system is properly challenged, the proffering party must offer evidence on this point [*see People v. Hawkins (2002) 98 CA4th 1428, 121 CR2d 627* (trial court did not err in rejecting defendant's hearsay objection and admitting printouts reflecting computer's internal operations into evidence)].



173 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
V. APPLYING THE SECONDARY EVIDENCE RULE TO ESI

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.31

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.31 Content of Writing May Be Proved by Otherwise Admissible Secondary Evidence in Most Cases.

15.31[1] Secondary Evidence Generally May Be Used to Prove Content of Writing. The content of a writing may be proved by otherwise admissible secondary evidence [*Evid Code § 1521(a)*]. The term "secondary evidence" is not specifically defined in the Evidence Code. Some categories mentioned in other sections of the Code include the following:

- Official records [*Evid Code § 1532*].
- Certified copies [*Evid Code § 1531*].
- Business records [*Evid Code § 1550*].
- Computer-stored documents [*Evid Code § 1552*].
- Oral testimony, if specifically authorized by statute [*Evid Code § 1523; see 15.32*].

Consider:

The purpose of the secondary evidence rule is to place the exact words or other contents of the original document before the court. Therefore, a counterpart that was created in the exact same manner serves equally as well as the original, if the counterpart is the product of a method that accurately reproduces the original. The California Evidence Code defines a duplicate as "counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic rerecording, or by chemical reproduction, or by other equivalent technique which accurately reproduces the original" [*Evid Code § 260*].



Strategic Point:

The status of the ESI as "original" or "secondary" evidence affects the foundational showing that must be

made to have the item admitted into evidence. If the ESI is original, the proffering party need only show the remaining four steps in order to have it admitted--it is relevant, authentic, does not contain impermissible hearsay, and is not unduly prejudicial [see 15.05[2]]. If the ESI is a duplicate, the proffering party also must show that it is "otherwise admissible secondary evidence" [Evid Code § 1521(a)]: that it is a true and correct copy of the original and that it was made using appropriate methods [see Evid Code § 1401(b) (authentication of secondary evidence required before it can be admitted)].



Warning:

The secondary evidence rule does not excuse compliance with authentication requirements [Evid Code § 1521(d); see 15.10-15.18].

15.31[2] Court Must Exclude Secondary Evidence of Writing Under Specified Circumstances.

Notwithstanding the general rule, the court must exclude secondary evidence of the content of writing if the court determines either of the following [Evid Code § 1521(a); see *Osswald v. Anderson* (1996) 49 CA4th 812, 57 CR2d 23 (genuine dispute existed as to terms of trust writing, invalidating proof of contents of writing by secondary means)]:

- A genuine dispute exists concerning material terms of the writing and justice requires the exclusion.
- Admission of the secondary evidence would be unfair.

In addition, the court in a criminal action is required to exclude secondary evidence of the content of a writing if the original is in the proponent's possession, custody, or control, and the proponent has not made the original reasonably available for inspection at or before trial, *unless* the evidence is one of the following [Evid Code § 1522(a)]:

- A duplicate [see Evid Code 260 (definition)].
- A writing that is not closely related to the controlling issues in the action.
- A copy of a writing in the custody of a public entity.
- A copy of a writing that is recorded in the public records, if the record or a certified copy of it is made evidence of the writing by statute.

When secondary evidence is excluded, the original is effectively required for admission into evidence [see 15.30[2]].



174 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
V. APPLYING THE SECONDARY EVIDENCE RULE TO ESI

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.32

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.32 Content of Writing May Be Proved by Oral Testimony Under Limited Circumstances.

The general rule is that oral testimony is *not* admissible to prove the content of a writing, except as provided by statute [*Evid Code* § 1523(a)]. However, statutory exceptions provide that oral testimony *is* admissible in the following circumstances:

- The proponent does not have possession or control of a copy of the writing and the original is lost or has been destroyed without fraudulent intent on the part of the proponent [*Evid Code* § 1523(b)].
- The proponent does not have possession or control of the original or a copy of the writing, and either of the following conditions is satisfied [*Evid Code* § 1523(c)]:
 - Neither the writing nor a copy of the writing was reasonably procurable by the proponent by use of the court's process or by other available means; or
 - The writing is not closely related to the controlling issues and it would be inexpedient to require its production.
- The writing consists of numerous accounts or other writings that cannot be examined in court without great loss of time, and the evidence sought from them is only the general result of the whole [*Evid Code* § 1523(d)].



175 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
VI. FORMS

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.33

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.33 Stipulation Regarding Admission of Items of ESI Into Evidence

Stipulation Regarding Admission of Items of ESI Into Evidence
SUPERIOR COURT OF CALIFORNIA,
COUNTY OF _____

_____, [name],
Plaintiff,
vs.
_____, [names],
Defendant.

STIPULATION REGARDING ADMISSION LIS-
TED ITEMS INTO EVIDENCE

IT IS HEREBY STIPULATED AND AGREED by and between the parties hereto, by their respective counsel, that, for the purpose of trial in this action the parties and each of them waive any objections to the entry of the listed exhibits into evidence in this matter.

The Exhibits subject to this stipulation are: _____ [list and briefly identify each item of ESI to which stipulation applies]

Undisputed facts are as follows:

1. _____ [list undisputed facts here and in subsequent numbered paragraphs].

2. _____.

3. _____.

Dated:_____ .

Attorney for Plaintiff

[*firm name, if any*]

By: _____ [*signature*]

_____ [*typed name*]

Date:_____ .

Attorney for Defendant

[*firm name, if any*]

By: _____ [*signature*]

_____ [*typed name*]

Date:_____ .

NOTES:

Authority:

See *CCP* § 283(1)



176 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial

VI. FORMS

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.34

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.34 Chain of Custody Record for ESI.

Chain of Custody Record for ESI.

[Click here to view image.](#)

Notes:

Attacking authenticity by showing faulty chain of custody: See 15.17[5]

Documentation of chain of custody: See 9.21



177 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
VI. FORMS

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.35

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.35 Sample Direct Examination Questions--Authenticating an E-Mail.

Q: Mr. Smith, I am handing you a copy of a document which has been marked as Defense Exhibit A for identification. Do you recognize this document?

A: Yes.

Q: How do you recognize the document?

A: I wrote this e-mail to Mr. James on December 2, 2008.

Q: Your Honor, I offer the e-mail as Defense Exhibit next in order.

NOTES:

Authority: *Evid Code §§ 1400, 1401, 1520*

Requirement for Authentication of ESI: See *15.12*

Methods of Proving Authenticity: See *15.15, 15.16*



178 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
VI. FORMS

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.36

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.36 Sample Direct Examination Questions--Authenticating an Electronic Record.

Q: Mr. Smith, does your employer record information about employee activity on the Internet?

A: Yes it does.

Q: How is that activity recorded?

A: We use a computer program to monitor Internet activity. It automatically logs or records each website an employee visits.

Q: How is this information stored?

A: The computer stores the date, time, employee name, and websites visited in a special file on the hard disk of our network.

Q: Who has access to that file?

A: Only the system manager has access to the file. The file is password protected and may not be accessed by any other user on the system.

Q: Who is the system manager?

A: I am.

Q: Are you familiar with the operation and use of the monitoring software?

A: Yes. I personally installed and configured the software. I am responsible for ensuring the logging information is properly recorded.

Q: Mr. Smith, I am handing you a computer printout, which has been marked as Defense Exhibit B for identification. Do you recognize this document?

A: Yes, I do.

Q: How do you recognize the document?

A: I prepared it.

Q: What does the exhibit represent?

A: This is a printout of a portion of the log file created by our Internet monitoring software.

Q: How was this printout prepared?

A: I directed our monitoring software to print out the Internet activity of employee Mike Jones on May 27, 2009.

Q: And is this exhibit a copy of the printout generated by the monitoring software?

A: Yes.

Q: Your Honor, I offer the printout as Defense Exhibit next in order.

NOTES:

Authority: *Evid Code §§ 1400, 1401, 1520*

Requirement for Authentication of ESI: See 15.12

Methods of Proving Authenticity: See 15.15, 15.16



179 of 179 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 15 Admissibility of Electronic Evidence at Trial
VI. FORMS

1-15 MB Practice Guide: CA E-Discovery and Evidence 15.37

AUTHOR: Diane E. Barry, Esq. Hon. James L. Smith (Ret.), Practice Consultant

15.37 Sample Direct Examination Questions--Direct Examination Admission of Party.

Q: Mr. Smith, I am handing you a printout of an e-mail, which has been marked as Defense Exhibit A for identification. Do you recognize this document?

A: Yes.

Q: How do you recognize the document?

A: I received this e-mail in response to an e-mail that I had sent to Mr. James.

Q: How do you know that this e-mail was in response to the message you had sent to Mr. James?

A: On September 14, 2008, I sent an e-mail to Mr. James inquiring about the status of our purchase agreement. I was concerned that our order had not been filled. The day after I sent my message, I received an e-mail from Mr. James stating that our purchase order would be filled within five business days.

Q: Does this Exhibit accurately reflect the message you received?

A: Yes. This is the printout of the message I made at your request using my company's e-mail software.

Q: Your Honor, I offer the printout as Defense Exhibit next in order.

Opposing Counsel: Objection. The e-mail is hearsay, not within any recognized exception.

Counsel: Your Honor, the e-mail is admissible as an admission of a party opponent.

Court: Objection overruled.

NOTES:

Authority: *Evid Code § 403(a)(4)*

Authentication by Admission of Party Opponent: See 15.15[3]



1 of 22 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 16 Establishing Best Practices Regarding Electronically Stored Information

1-16 MB Practice Guide: CA E-Discovery and Evidence 16.syn

AUTHOR: Diane E. Barry, Esq.

§ 16.syn Synopsis to Chapter 16: Establishing Best Practices Regarding Electronically Stored Information

16.01 Scope.

16.02 Objective and Strategy.

16.03 CHECKLIST: Planning for Document Retention Program.

16.04 Options and Strategies.

16.05 Organization Should Establish Interdepartmental Work Group to Formulate Program.

16.06 Work Group Should Determine Objectives of Document Retention Program.

16.06[1] Program Should Reflect Organization's Business Objectives.

16.06[1][a] Maintaining Unnecessary Information Is Costly.

16.06[1][b] Organization May Legitimately Restrict Use of Outdated Information.

16.06[2] Program Should Reflect Organization's Legal Requirements and Objectives.

16.06[2][a] Program Should Comply With Applicable Retention Requirements.

16.06[2][b] Program Should Minimize Potential Litigation Risk and Costs.

16.06[2][c] Program Should Facilitate Defending Against Claims of Spoliation and Bad Faith Destruction of Information.

16.06[3] Program Should Reflect Organization's Information Technology Needs.

16.06[3][a] Most of Burden of Document Retention Program Will Be Borne by Information Technology Department.

16.06[3][b] Information Technology Department Needs Sufficient Resources for Storage and Management.

16.06[3][c] Information Technology Department Must Understand Business and Legal Objectives of Document Retention Program.

16.07 CHECKLIST: Creating Document Retention Program.

16.08 Options and Strategies.

16.09 Document Retention Program Should Include Document Retention Policy.

16.09[1] Work Group Should Formulate Document Retention Policy.

16.09[2] Document Retention Policy Must Categorize Data by Subject Matter, Not by Storage Media.

16.09[3] Document Retention Policy Must Address Both Paper and Electronic Data.

16.09[4] Document Retention Policy Must Establish Retention Periods.

16.09[5] Document Retention Policy Should Address Non-Documentary Retention Needs.

16.10 Document Retention Program Should Include Document Retention Schedule.

16.10[1] Document Retention Schedule Implements Document Retention Policy.

16.10[2] Document Retention Schedule Should List Categories of Information.

16.10[2][a] List Should Be Specific.

16.10[2][b] Automated Categorization May Provide Starting Point.

16.10[2][c] Manual Categorization Will Be Necessary for Most Paper Documents.

16.10[3] Document Retention Schedule Should Specify Retention Periods.

16.10[4] Document Retention Schedule Should Designate Retention Custodians.

16.11 Document Retention Program Should Include Implementation Plan.

16.11[1] Implementation Plan Provides Instructions for Custodians.

16.11[2] Implementation Plan Should Specify Timing.

16.11[3] Implementation Plan Should Include Data Destruction Protocols.

16.11[4] Implementation Plan Should Provide Special Procedures for Sensitive or Confidential Information.

16.12 Document Retention Program Should Include Rollout Plan.

16.12[1] Proper Rollout Is Important to Success of Program.

16.12[2] Rollout in Large Organization Typically Is Done Incrementally.

16.12[3] Rollout Must Not Disturb Existing Litigation Holds.

16.13 Document Retention Program Should Include Compliance Program.

16.13[1] Compliance Program Helps Ensure Effectiveness of Document Retention Program.

16.13[2] Compliance Program Should Include Education Component.

16.13[3] Compliance Program Should Require Custodian Certifications.

16.13[4] Compliance Program Should Require Periodic Audits.

16.13[5] Compliance Program Should Include Periodic Review.

16.14 CHECKLIST: Making Use of Document Retention Program in Discovery.

16.15 Options and Strategies.

16.16 Organization May Use Its Document Retention Program in Responding to Discovery Demand.

16.16[1] Document Retention Program Assists in Preventing Loss of Responsive Information.

16.16[1][a] Organization Has Duty to Preserve Materials Relevant to Litigation.

16.16[1][b] Document Retention Schedule Provides Starting Point for Litigation Hold or Responding to Discovery Demands.

16.16[2] Document Retention Program Provides Basis for Good Faith Defenses.

16.17 Opposing Party May Use Organization's Document Retention Program to Obtain Discovery.

16.17[1] Document Retention Schedule May Assist in Identifying Discoverable Information.

16.17[2] Document Retention Program May Provide Basis for Inference of Bad Faith.

16.18 Sample Document Retention Policy.

16.19 Sample Document Retention Schedule.

16.20 Sample Protocol for Destruction of Sensitive Paper Documents.

16.21 Sample Data-Wipe Protocol for Hard Drives.

Diane E. Barry, Esq. n*

FOOTNOTES:

(n7)Footnote *. Diane E. Barry, Esq., is the Director of Discovery Strategy & Management at International Litigation

Services, Inc. Diane's practice focuses on discovery of electronically stored information (ESI) under state and federal rules of civil procedure, and complex litigation discovery planning and management. Diane assists clients in planning and preparing for ESI discovery conferences and court appearances, as well as preparation for specialized discovery such as information technology (IT) custodian depositions, and key player and IT interviews. In addition, Diane has significant expertise in utilizing technology to improve results in privilege and relevance review. Diane earned her A.B. degree from Vassar College and her J.D. degree, cum laude, from the Boston University School of Law. She holds a professional certification in Data Warehousing from U.C. Berkeley.



2 of 22 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 16 Establishing Best Practices Regarding Electronically Stored Information

I. STRATEGY

1-16 MB Practice Guide: CA E-Discovery and Evidence 16.01

AUTHOR: Diane E. Barry, Esq.

16.01 Scope.

This chapter covers the essential aspects of document retention for attorneys engaging in discovery of electronically stored information, including:

- Planning for a document retention program [see 16.0316.06].
- Creating and implementing a document retention program [see 16.07-16.13; Forms: see 16.18-21].
- Making use of a document retention program in discovery [see 16.14-16.17].

This chapter does not cover the procedures for responding to a demand for production of electronically stored information. For discussion of those procedures, see Ch. 8, Responding to Electronic Discovery Demands in California.

This chapter does not cover the procedures for gathering and producing electronically stored information. For discussion of those procedures, see Ch. 9, Gathering and Producing Electronically Stored Information.

This chapter does not cover the procedures for opposing a demand for production of electronically stored information. For discussion of those procedures, see Ch. 10, Opposing Demands for Production of Electronic Evidence in California Court.

Core Statutes:

18 USC §§ 1519-1520; CCP § 2023.010(d), (g), (h); Cal Rules Prof Conduct, Rule 5-220.



3 of 22 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 16 Establishing Best Practices Regarding Electronically Stored Information

I. STRATEGY

1-16 MB Practice Guide: CA E-Discovery and Evidence 16.02

AUTHOR: Diane E. Barry, Esq.

16.02 Objective and Strategy.

A general understanding of the issues and regular practices in the area of document retention is useful for counsel representing a client that wishes to establish a document retention program or that must engage in the discovery of electronically stored information.

As a matter of sound business operations, a good program for document retention (and the associated destruction of documents) saves time and money. An organization can be overwhelmed by the amount of information it creates and stores unless there is a protocol for periodically weeding out outdated information [see Excerpt, Report of Judicial Conference Committee on Rules of Practice & Procedure to Chief Justice of United States and Members of Judicial Conference of United States 14 (Sept. 2005) ("[T]he regular purging of e-mails or other electronic communications is necessary to prevent a build-up of data that can overwhelm the most robust electronic information systems."), *available at* http://www.uscourts.gov/rules/supct1105/Excerpt_STReport_CV.pdf]. Although storage may be inexpensive, retrieval of electronically stored information takes time, planning, personnel, and budget dollars. If there is less information, there is less to plan for, index, store, and retrieve. Thus, a good document retention program weeds out what does not need to be kept, and it appropriately archives what should be kept in a manner that facilitates efficient retrieval.

Cross References:

Discussion of planning for a document retention program, see 16.03-16.06.

Discussion of elements of document retention program, see 16.07-16.13.

From the litigation standpoint, a litigation budget can choke on the costs imposed by poor document retention. If the client's stored information is not appropriately indexed, counsel must review all of the available information to make sure it does or does not pertain to a particular litigation matter. In a world where 80 percent or more of a discovery budget can go to pay first-pass review expenses, the costs of inefficient storage habits can mount up quickly. If the client's information is appropriately indexed, counsel can eliminate entire groups of data from this process, reducing the amount of electronically stored information that goes into the review, thus reducing overall discovery costs. For the opposing party, early discovery of the organization's document retention program can serve as a useful tool for planning further discovery.

 Cross Reference:

Discussion of document retention program as resource in planning and responding to discovery, see 16.14, 16.15, 16.16[1][b], 16.17[1].

Finally, a good document retention program is good risk management. The organization bears the ultimate responsibility for spoliation, even if the electronically stored information or other materials are not intentionally destroyed. If the organization was responsible for retaining them, and the documents were destroyed after the duty to preserve attached, sanctions may be imposed [see *New Albertsons, Inc. v. Superior Court* (2008) 168 CA4th 1403, 1429-1430, 86 CR3d 457, 477-478 ; see CCP § 2023.030]. A good document retention schedule speeds the litigation hold process. Counsel will know what information the client possesses, who is responsible for destroying it, and whom to contact to halt destruction and commence litigation hold procedures. In the case of truly inadvertent destruction, a good retention program assists the organization in showing good faith despite the existence of problems with a production [see CCP §§ 1985.8(l)(2), 2031.060(i)(2), 2031.300(d)(2), 2031.310(j)(2), 2031.320(d)(2)].

**Warning:**

Not having a coherent organization-wide document retention program, and relying on employees to self-archive their own electronically stored information, does not constitute a good-faith retention policy and may subject the organization to sanctions if documents relevant in litigation are lost [*Philip M. Adams Assocs., L.L.C. v. Dell, Inc.* (D Utah 2009) 621 F Supp2d 1173 (finding that the safe harbor of Fed R Civ P 37(e) did not apply to prevent sanctions)].

 Cross Reference:

Discussion of duty to preserve relevant documents, see 16.16[1][a]. Discussion of document retention program as factor in establishing good faith of organization, see 16.16[2], 16.17[2].



4 of 22 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 16 Establishing Best Practices Regarding Electronically Stored Information

II. PLANNING FOR DOCUMENT RETENTION PROGRAM

1-16 MB Practice Guide: CA E-Discovery and Evidence 16.03

AUTHOR: Diane E. Barry, Esq.

16.03 CHECKLIST: Planning for Document Retention Program.

☐ Form interdepartmental work group to plan document retention program, including representatives from following departments of organization:

Discussion:

See 16.05

- ☐ Business operations.
- ☐ Human resources.
- ☐ In-house or outside legal counsel.
- ☐ Information technology.
- ☐ Risk management.
- ☐ Records management.

☐ Have interdepartmental work group identify organization's business objectives that should be reflected in document retention program.

Discussion:

See 16.06[1]

☐ Have interdepartmental work group identify legal requirements and objectives that must be met by document retention program, including following:

Discussion:

See 16.06[2]

☐ Have interdepartmental work group identify organization's information technology objectives and objectives and budgeting needs that should be reflected in document retention program.

Discussion:

See 16.06[3]

☐ Have interdepartmental work group obtain documentation of any document retention programs or policies previously adopted by organization or any of its departments or divisions.

☐ Have interdepartmental work group review circumstances of any previous instance in which organization was legally sanctioned for failure to preserve information relevant to litigation.

Discussion:

See 16.16[1][a]

☐ Have interdepartmental work group review determine whether organization is currently engaged in litigation or is facing imminent litigation.

Discussion:

See 16.16[1][a]



5 of 22 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 16 Establishing Best Practices Regarding Electronically Stored Information

II. PLANNING FOR DOCUMENT RETENTION PROGRAM

1-16 MB Practice Guide: CA E-Discovery and Evidence 16.04

AUTHOR: Diane E. Barry, Esq.

16.04 Options and Strategies.

A document retention program should be designed to reflect and support an organization's business objectives, the legal requirements the organization must meet (including human resources requirements), and the needs of its information technology department. Planning for the program, therefore, should include participation by all of those departments or divisions, as well as other significant units such as risk-management and records-management departments.

Cross References:

Discussion of formation of interdepartmental work group to plan for document retention program, see 16.05.

Discussion of objectives and requirements that should be reflected in document retention program, see 16.06.

Creating an effective document retention program is a project that requires time and careful planning. Such a project should, if possible, be undertaken at a time when there is no pending litigation or government investigation that might restrict the organization's ability to purge outdated documents and information. Creation and implementation of a document retention program is still possible while the organization is engaged in active litigation or is under government investigation, but extreme caution must be exercised during rollout of the program to avoid destruction of material that is outdated from a business standpoint but remains relevant to the litigation or investigation.

Cross References:

Discussion of rollout of document retention program, see 16.12.

Discussion of duty to preserve materials during imminent or pending litigation, see 16.12[3], 16.16[1][a].



6 of 22 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 16 Establishing Best Practices Regarding Electronically Stored Information

II. PLANNING FOR DOCUMENT RETENTION PROGRAM

1-16 MB Practice Guide: CA E-Discovery and Evidence 16.05

AUTHOR: Diane E. Barry, Esq.

16.05 Organization Should Establish Interdepartmental Work Group to Formulate Program.

To create a successful document retention program, an organization should establish a work group composed of representatives from at least the following departments or divisions: business operations, human resources, legal (in-house and often outside counsel as well), and information technology. If the organization also has a risk-management or records-management department, they should also be included. The participants in the work group will need to meet to discern the initial needs of the organization with regard to its records and to create the initial program (including rollout).

A similar group will be needed for ongoing review and maintenance of the program.



Cross Reference:

Discussion of ongoing review and maintenance of document retention program, see 16.13[5].



7 of 22 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 16 Establishing Best Practices Regarding Electronically Stored Information
II. PLANNING FOR DOCUMENT RETENTION PROGRAM

1-16 MB Practice Guide: CA E-Discovery and Evidence 16.06

AUTHOR: Diane E. Barry, Esq.**16.06 Work Group Should Determine Objectives of Document Retention Program.****16.06[1] Program Should Reflect Organization's Business Objectives.**

16.06[1][a] Maintaining Unnecessary Information Is Costly. Storage, indexing, maintenance, and retrieval of electronically stored information all cost money and valuable staff time. While the organization needs the information, this is money well spent. Once the information is past its useful life, the costs of maintaining it should be saved by disposing of the information responsibly. It is not wrong for a business to have a policy of destroying documents after the point when there is no good business reason to retain them [see *Arthur Andersen LLP v. United States* (2005) 544 US 696, 704, 125 S Ct 2129, 161 L Ed2d 1008 ; *Fid. Nat'l Title Ins. Co. v. Intercounty Nat'l Title Ins. Co.* (7th Cir 2005) 412 F3d 745, 751 ("[t]here is no legal duty to be a pack rat"); *Cedars-Sinai Medical Center v. Superior Court* (1998) 18 C4th 1, 74 CR2d 248, 954 P2d 511 (refusing to recognize a spoliation tort in part because it would impose costs by forcing organizations to take extraordinary measures to retain documents of no apparent value)].

16.06[1][b] Organization May Legitimately Restrict Use of Outdated Information. Document retention programs created in part to keep certain information from getting into the hands of others, including the government, are common in business. It is not wrongful for an organization to require its employees to comply with such a program "under ordinary circumstances." [*Arthur Andersen LLP v. United States* (2005) 544 US 696, 704, 125 S Ct 2129, 161 L Ed2d 1008] .

**Warning:**

The destruction of relevant information after the commencement of a litigation or in anticipation of a discovery request is sanctionable as a misuse of the discovery process [*New Albertsons, Inc. v. Superior Court* (2008) 168 CA4th 1403, 1429-1430, 86 CR3d 457, 477-478 ; see CCP § 2023.030].

**Cross References:**

Discussion of duty to preserve evidence relevant to litigation, see 16.16[1][a].

Litigation holds and preservation demands, see *Ch. 5, Initial Procedures in E-Discovery: Notice*,

Document Preservation, Meeting and Conferencing, and Case Management Conference, 5.03-5.13.

16.06[2] Program Should Reflect Organization's Legal Requirements and Objectives.

16.06[2][a] Program Should Comply With Applicable Retention Requirements. In planning for a document retention program, the interdepartmental work group should consider any retention periods imposed by statute, regulation, or contract.

Examples--Retention Periods Imposed by Law:

Retention periods imposed by law include the following:

- The Sarbanes-Oxley Act 2002 (sometimes called "SOX") [Pub L No 107-204, 116 Stat 745 (codified in scattered sections of 11, 15, 18, 28, & 29 U.S.C.)] imposes requirements on publicly held companies and their accounting and auditing firms regarding the retention and destruction of various financial records. For example, under SOX it is a crime to destroy, alter, or falsify records with the intent to impede, obstruct, or influence a federal investigation or bankruptcy proceeding [18 USC § 1519]. It is also a crime to destroy certain records of an audit of a corporation that issues securities subject to section 10A(a) of the Securities Exchange Act of 1934 [see 18 USC § 1520 (audit records must be retained for five years after end of fiscal period in which audit was completed); see also 15 USC § 78j-1(a); but see 17 CFR § 210.2-06 (imposing seven-year retention period for audit records)].

- The Internal Revenue Service (IRS) requires that businesses keep employment tax records for a minimum of four years. If there are claims of serious errors (unreported income of more than 25 percent of the income reported), the IRS reserves the right to audit returns up to six years. If a business files a claim of loss from worthless securities, or a bad debt deduction, the retention period jumps to seven years [see IRS Pub. 583 (1/2007), Starting a Business and Keeping Records, Table 3].

- Securities and Exchange Commission (SEC) regulations require that exchange members, brokers, and dealers preserve specified transaction and other records for not less than six years. For at least the first two years, the records must be in "an easily accessible place" [17 CFR §§ 240.17a-3, 240.17a-4].

- If the organization engages in a regulated activity, there may be retention requirements associated with that activity. For example, the owner or operator of a facility that handles or stores toxic waste must retain all records that pertain to a conditional authorization permit for at least five years [Health & Safety Code § 25200.3(c)(7)].

Examples--Contractual Retention Requirements:

Contracts can require the retention of all or particular documents. For example, it is not uncommon for a large-scale construction project to require the retention of all documents related to change orders for a year or more after the construction is completed. Government manufacturing contracts often require retention of contract, quality assurance, and accounting records for a period after the close of the contract.

16.06[2]b] Program Should Minimize Potential Litigation Risk and Costs. Many organizations have risk management departments or programs. The purpose of such departments or programs is to analyze the organization's exposure to risk, and to create conditions that will best handle that exposure. A document retention program is a useful risk management tool. If the organization becomes involved in litigation, the costs of review of outdated information for discovery purposes can be extreme; document review costs can exceed 80 percent of a discovery budget. The risk of paying for unnecessary document review can be minimized through good retention practices.

16.06[2][c] Program Should Facilitate Defending Against Claims of Spoliation and Bad Faith Destruction of Information. The destruction of relevant information after the commencement of litigation or in anticipation of a discovery request is sanctionable as an abuse of discovery [*New Albertsons v. Superior Court* (2008) 168 CA4th 1403, 1429-1430, 86 CR3d 457, 477-478 ; see CCP § 2023.030]. A good document retention program, and in particular a good document retention schedule, provides an organization with a reliable way to institute a litigation hold. It can also provide evidence of good faith (or at least the absence of bad faith) if documents are inadvertently destroyed after the organization becomes duty-bound to retain them [see CCP §§ 1985.8(l)(1), 2031.060(i)(1), 2031.300(d)(1), 2031.310(j)(1), 2031.320(d)(1)].



Cross Reference:

Discussion of litigation hold, see 16.16[1].

Examples--Document Retention Program Can Prevent Finding of Bad Faith Destruction of Evidence:

The existence of a well-designed document retention program helped prevent a finding of bad faith in the following cases:

- A chemist sued a food products company, alleged that the defendant had misappropriated the plaintiff's trade secrets, formulas useful in making bread. Product history cards produced by the defendant did not show the recipe changes alleged by the plaintiff. There was also no evidence to support the plaintiff's claim that the defendant had altered the recipe cards or destroyed other relevant evidence regarding the recipes. The defendant offered evidence that any missing materials had been destroyed or discarded in the normal course of business as part of its document retention program. In the face of this evidence, the court concluded that the plaintiff's unsupported accusations were insufficient to support a finding that the evidence had been destroyed in bad faith [*Kim v. Dawn Food Prods., Inc.* (7th Cir 2006) 206 Fed Appx 558, 560] .

- In an employment discrimination case, one of the reasons given by the employer for terminating the plaintiff's employment was his falsification of documents, including a work order. The work order was not preserved for litigation. The court held that the mere fact of the destruction did not warrant an adverse jury instruction, as it had been destroyed as part of the regular retention program of the employer, and thus had not been destroyed in bad faith [*Martinez v. Abbott Labs.* (7th Cir 2006) 171 Fed Appx 528, 531] .



Warning:

Even if a document retention program is neutral on its face, the circumstances surrounding its application may demonstrate bad faith. If documents relevant to a litigation matter or government investigation are destroyed before they can be produced, a court can consider whether the application of the retention policy to the missing documents was reasonable under the circumstances, or whether the policy was applied in bad faith [see *Lewy v. Remington Arms Co.* (8th Cir 1988) 836 F2d 1104, 1112 ; *Phillip M. Adams & Assocs., L.L.C. v. Dell, Inc.* (D Utah 2009) 2009 US Dist LEXIS 26964 ("[a] court--and more importantly, a litigant--is not required to simply accept whatever information management practices a party may have. A practice may be unreasonable, given responsibilities to third parties. While a party may design its information management practices to suit its business purposes, one of those business purposes must be accountability to third parties. For example, a recreation park's policy to destroy records at the end of each season--prior to the running of the applicable statute of limitations for injuries--has been held to entitle the plaintiff to an adverse inference instruction")].

Example--Bad Faith Application of Document Retention Program:

Defendant filed for and received a patent. As part of its business plan, the company decided to sue industry members to create a "patent minefield" and to interest the other companies in simply licensing its technology. The defendant company was also sure that key industry players were actually infringing on its patent. As part of its efforts to get ready for the planned litigation, the company created and implemented a "Document Retention/Destruction Program." The company scheduled "Shred Days," during which employees destroyed documents in compliance with the new policy. The outside company hired to shred the documents on the first such "Shred Day" estimated that they destroyed more than 400 bankers' boxes of materials that first day. Three hundred boxes were shredded on another day. The defendant had its outside counsel clean its files of any patent prosecution documents that were not part of the official record. The court ruled that under these circumstances, the defendant's retention program was instituted in bad faith; as a sanction the court held that patents in question were unenforceable as against the plaintiffs [*Micron Tech., Inc. v. Rambus Inc. (D Del 2009) 255 FRD 135, 148-149*] .

16.06[3] Program Should Reflect Organization's Information Technology Needs.

16.06[3][a] Most of Burden of Document Retention Program Will Be Borne by Information Technology Department. The information technology department (IT) will bear most of the burden of an organization's document retention program. Today, most information begins its life on a computer, even if it is later produced in printed form, and most information is never reduced to paper. Therefore, IT will be in charge of the storage, maintenance, and retrieval of much of an organization's information. It is also true that IT tools can speed almost every task associated with the retention program.

Examples:

The ways in which IT can facilitate the creation and implementation of a document retention program include the following:

- Computer tools can create category lists by crawling the organization's network and reviewing content.
- Tools such as the EnCase forensic software from Guidance Software can be used to search a network for specific information, and either mark its place or retrieve it.
- Wipe/eradication tools can remove outdated files from hard drives or networks.
- Archiving software provides tools for storing and searching corporate ESI, and eventually deleting it in accordance with regulatory requirements and the organization's retention policies.

Consider:

IT's engagement in and commitment to a document retention process is invaluable. However, IT needs support from the organization's business units and cannot be expected to take on the entire process by itself. For example, IT cannot determine appropriate retention periods, which must be set on the basis of the requirements identified by the business operations and legal departments.

16.06[3][b] Information Technology Department Needs Sufficient Resources for Storage and Management.

The retention program will have a direct impact on IT's budget. Computer storage costs for hardware such as servers and removable hard drives usually come out of the IT budget. The costs for staff to maintain servers and networks and archives often come out of the IT budget. As systems change, IT must often provide support for the new system and the legacy system (e.g., keeping old hardware, software, and manuals for dealing with earlier systems). Thus, IT is the most likely entity to understand the costs associated with keeping old data. IT can help quantify both the costs of keeping old data, and the costs of implementing a particular retention or destruction method.

16.06[3][c] Information Technology Department Must Understand Business and Legal Objectives of Document Retention Program. The business and legal objectives of the document retention program must be understood by IT, so that IT in its own operations will not undermine the program.

Example:

When a new computer system or software is installed, IT needs to understand how the new system or software will affect the operation of the document retention program. For example, old data--generated under the old computer system or program--may need to be retained for a few years to meet regulatory requirements. In such a case, if the old data requires the old computer program to work properly, then the old program should be kept along with the data. It also is helpful if at least some staff know how to use the old program.



8 of 22 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 16 Establishing Best Practices Regarding Electronically Stored Information

III. CREATING DOCUMENT RETENTION PROGRAM

1-16 MB Practice Guide: CA E-Discovery and Evidence 16.07

AUTHOR: Diane E. Barry, Esq.

16.07 CHECKLIST: Creating Document Retention Program.

- ☐ Formulate organization's document retention policy.

Discussion:

See 16.09[1]

- ☐ Categorize information by subject matter, not by storage media.

Discussion:

See 16.09[2]

- ☐ Address both paper and electronically stored information.

Discussion:

See 16.09[3]

- ☐ List retention period for each category of information.

Discussion:

See 16.09[3]

- ☐ Address any non-documentary retention needs.

Discussion:

See 16.09[4]

- ☐ Prepare document retention schedule.

Discussion:

See 16.10[1]

- ☐ List categories of information as specifically as possible.

Discussion:

See 16.10[2]

- ☐ Specify retention period for each category of information.

Discussion:

See 16.10[3]

- ☐ Designate custodian for each category of information.

Discussion:

See 16.10[4]

- ☐ Prepare implementation plan.

- ☐ Include instructions for custodians.

Discussion:

See 16.11[1]

- ☐ Specify timing for each action custodian must take.

Discussion:

See 16.11[2]

- ☐ Include data-destruction protocols.

Discussion:

See 16.11[3]

- ☐ Include any special procedures applicable to sensitive or confidential information.

Discussion:

See 16.11[4]

- ☐ Roll out document retention program.

Discussion:

See 16.12[1]

- ☐ Consider proceeding incrementally if organization is large.

Discussion:

See 16.12[2]

- ☐ Delay rollout for any department or division whose information is currently subject to litigation hold.

Discussion:

See 16.12[3]

- ☐ Formulate and implement ongoing compliance program, including following components:

Discussion:

See 16.13[1]

- ☐ Employee education.

Discussion:

See 16.13[2]

- ☐ Custodian certification requirements.

Discussion:

See 16.13[3]

- ☐ Periodic audits.

Discussion:

See 16.13[4]

- ☐ Periodic review of document retention program.

Discussion:

See 16.13[5]



9 of 22 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 16 Establishing Best Practices Regarding Electronically Stored Information

III. CREATING DOCUMENT RETENTION PROGRAM

1-16 MB Practice Guide: CA E-Discovery and Evidence 16.08

AUTHOR: Diane E. Barry, Esq.

16.08 Options and Strategies.

An effective document retention program should include the following elements: a document retention policy, a document retention schedule, an implementation plan, a rollout plan, and a compliance plan to ensure ongoing effectiveness of the program.

Cross References:

Discussion of document retention policy, see 16.09.

Discussion of document retention schedule, see 16.10.

Discussion of implementation plan, see 16.11.

Discussion of rollout plan, see 16.12.

Discussion of compliance plan, see 16.13.



10 of 22 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 16 Establishing Best Practices Regarding Electronically Stored Information
III. CREATING DOCUMENT RETENTION PROGRAM

1-16 MB Practice Guide: CA E-Discovery and Evidence 16.09

AUTHOR: Diane E. Barry, Esq.

16.09 Document Retention Program Should Include Document Retention Policy.

16.09[1] Work Group Should Formulate Document Retention Policy. The interdepartmental work group appointed to create the document retention program should establish the organization's document retention policy. A document retention policy lists by category all information created or maintained by the organization, together with the retention period for each category. The retention policy should address all retention needs of the organization. To formulate the document retention policy, the interdepartmental work group must research and generate the following information:

- An inventory of all categories of information (not categories of media) created and maintained by the organization.
- For each category of information in the inventory, the media or forms in which it is created or maintained (e.g., electronically stored information, paper documents).
- The physical location of every form of information in each category listed on the inventory.
- The useful business life of each category of information listed in the inventory. This is usually a matter for the business operations participants to determine.
- The legal retention requirements for each category of information listed in the inventory. These requirements can be statutory, regulatory, or contractual, and they are usually a matter for in-house and outside counsel to determine.
- Whether new software or hardware systems are needed or desired to assist in implementing the document retention policy.



Cross References:

Discussion of interdepartmental work group, see 16.05.

Discussion of need to address data by subject matter, see 16.09[2].

Discussion of need to address both paper documents and electronically stored information, see 16.09[3].

Discussion of retention periods, see 16.09[4].

Sample document retention policy, see 16.18.

Discussion of software and hardware systems for categorization of ESI and implementation of document retention, see 16.10[2][b].

Consider--Every Client Has Different Retention and Destruction Needs:

Counsel participating in the drafting of a document retention policy should bear in mind that document retention policies are usually client-specific documents. Some considerations are common to all entities; for example, most entities file tax returns and therefore need to retain tax-related records for similar periods of time. However, almost every business has specific circumstances that make its requirements different from others. For example, the retention and destruction periods for a health care clinic will differ from those for a surfboard repair shop. As another example, the natural business life of information is shorter for a marketing company than it is for a toxic waste disposal company. In this area of practice, therefore, counsel should be wary of using general forms without carefully tailoring them to the client's specific needs.

16.09[2] Document Retention Policy Must Categorize Data by Subject Matter, Not by Storage Media. The retention period specified for documents in each category of information must be selected based on the documents' content, not on the type of storage media. Retention periods apply to categories of information, not to categories of storage media. Thus, an organization cannot simply decide to retain all e-mails for two years, all paper documents for five years, and so forth, because a given e-mail or document might be subject to different legal requirements, depending on its subject matter.

16.09[3] Document Retention Policy Must Address Both Paper and Electronic Data. A good retention program must encompass both electronic and physical storage media, addressing the content rather than the media used to present the information.

Networked data is the easiest information to locate, categorize, set retention requirements for, and archive or delete. Appropriate computer tools can be set to the task using the searchable and malleable aspects of data to speed the tasks. Paper documents require more work, as people need to read and analyze information in order to categorize it, and archiving or destruction must be processed manually.

16.09[4] Document Retention Policy Must Establish Retention Periods. For each category of information, the retention period should be based on the useful business life of the information, or the legally required retention period, whichever is longer. The documentation for a retention schedule should include a listing of the authorities (e.g., a governing statute or a particular business condition) for each retention period. If it is not desirable to list these in the actual document retention policy document itself, the authorities ought to be listed in an accompanying memorandum. This listing will provide a starting place for revising and updating the retention schedule and eliminate the need to start from scratch each time the policy is revisited. The savings in legal fees can be substantial.

16.09[5] Document Retention Policy Should Address Non-Documentary Retention Needs. Not all corporate retention needs pertain to information on paper or electronic form. Many organizations have things and substances that require specialized handling and retention. A thorough retention policy will address the retention and appropriate disposal of these items as well as informational media.

Examples:

If the organization has submitted samples of its products, for example to a buyer or to a government agency, the organization may be required by contract or by regulations to keep the samples for a time. Organizations that store petroleum and other hazardous or toxic substances are often required to perform soil sampling or other testing. Such samples need to be retained for a time.



11 of 22 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 16 Establishing Best Practices Regarding Electronically Stored Information

III. CREATING DOCUMENT RETENTION PROGRAM

1-16 MB Practice Guide: CA E-Discovery and Evidence 16.10

AUTHOR: Diane E. Barry, Esq.

16.10 Document Retention Program Should Include Document Retention Schedule.

16.10[1] Document Retention Schedule Implements Document Retention Policy. A document retention schedule should implement the document retention policy by setting forth the following:

- A list of the information inventory, broken down to manageable units such as information category or physical location.
- For each identified information unit, a specification of its category in the document retention policy, and its associated retention period.
- For each category or physical location, a designation of an individual or individuals who will serve as custodians responsible for the retention and destruction of relevant information.

➡ **Cross References:**

Discussion of document retention policy, see 16.09.

Sample document retention policy, see 16.18.

16.10[2] Document Retention Schedule Should List Categories of Information.

16.10[2][a] List Should Be Specific. A document retention schedule must list each category of information (rather than listing types of media) with enough specificity for the custodian to decide what category a given document or piece of data belongs in.

Example:

Instead of listing "2008 e-mail," a document retention schedule should say something like "2008 State of California Corporate Tax Return Backup." This will allow the custodian to determine the appropriate category for an e-mail that documents an item in the 2008 tax return.

 Cross Reference:

Discussion of need to classify information by content rather than by storage media, see 16.09[2].

16.10[2][b] Automated Categorization May Provide Starting Point. There are useful categorization tools available that can be loaded to an organization's computer network, or attached through a separate utility. The tool set can crawl the network to seek out all information stored on the network, whether structured or unstructured; review and comprehend its content; and suggest categories to describe the groups of information found. The organization's working group creating the document retention program can then adjust, expand, or contract any of the categories suggested by the tool. The categories can be set to be broad or granular, as desired.

Examples:

Two examples of automated categorization tools are Autonomy (www.autonomy.com) and Stored IQ (www.storediq.com).

Consider:

An automated categorization tool can facilitate one of the more difficult tasks in the process of creating a document retention program. Also, once electronically stored information has been properly categorized, most of the same categories can be applied to paper documents. The mechanized effort can give a substantial leg up on the manual effort required to categorize paper records.

Consider:

Software in the area of ESI archiving and retention continues to evolve, and some tools go beyond categorization to also enable storage, search, e-discovery production, and implementation of document retention deletion policies.

16.10[2][c] Manual Categorization Will Be Necessary for Most Paper Documents. Essentially all of the various documents, file folders, file cabinets, archive boxes, and related items in the custody or control of the organization have to be put into retention categories so that a retention period can be assigned to them. Manual categorization is usually accomplished by the employees who create and maintain the paper documents.

Consider:

The task of manual categorization is made easier if a list of categories can be provided to the employees, who can supplement the list if they have trouble fitting particular documents into the categories provided. A basic list of categories created by an automated categorization tool for the organization's electronically stored information can be used for this purpose.

 Cross Reference:

Discussion of automated categorization tools, see 16.10[2][b].

16.10[3] Document Retention Schedule Should Specify Retention Periods. The retention schedule should specify for each category of information the retention period established in the document retention policy.

 Cross Reference:

Discussion of establishing retention periods, see 16.09[4].

16.10[4] Document Retention Schedule Should Designate Retention Custodians. Generally, the person responsible for shredding or deleting a given document should be someone other than the person who owns the document during its useful lifetime. The person who owns the document has a tendency to want to hold onto it. For electronic documents, the deletion can be mechanized, and the "custodian" should be a person who understands the deletion system sufficiently well to turn it off or to adjust it as needed. This means this person is usually IT staff. For

paper documents, many organizations choose a custodian for each group or department.



Strategic Point:

Custodians should be persons with sufficient authority to carry out the document retention program. If a custodian comes to collect files for destruction, if the document owners can ignore them, the program will fail. Similarly, with electronically stored information, if someone can order the custodian to omit someone's files from a scheduled deletion, the program will fail. Therefore, each custodian must either have sufficient position that the staff will not want to ignore or coerce the custodian, or the staff must know that the organization stands behind the custodian's work.



12 of 22 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 16 Establishing Best Practices Regarding Electronically Stored Information

III. CREATING DOCUMENT RETENTION PROGRAM

1-16 MB Practice Guide: CA E-Discovery and Evidence 16.11

AUTHOR: Diane E. Barry, Esq.

16.11 Document Retention Program Should Include Implementation Plan.

16.11[1] Implementation Plan Provides Instructions for Custodians. The implementation plan should look like a manual for the custodians. It should instruct custodians regarding what should be done when the time limit has come for particular information assigned to them for destruction, and what certification paperwork should be generated.

16.11[2] Implementation Plan Should Specify Timing. The plan must provide for timing of when the custodian should take various actions. A timing protocol appropriate for the organization's size and complexity should be created.

Examples:

An implementation plan might, for example, provide for the destruction of data immediately upon the information reaching the end of its retention period. Alternatively, it might provide for monthly, bi-monthly, or annual destruction of data that has reached the end of its retention period since the last mandated destruction. Some large organizations have an official date once or twice a year when their employees organize their files and certify compliance with the document retention policy.



Cross Reference:

Discussion of data destruction protocols, see *16.11[3]*.

16.11[3] Implementation Plan Should Include Data Destruction Protocols. Implementation of a document retention policy requires specific instruction on the appropriate destruction of each kind of storage media the custodians are responsible for, such as paper, hard drives, and data located on the network, CD-ROMs, and USB drives. The plan should specify what steps the custodian must take to fulfill their duties to eradicate the information. If they are personally responsible for the eradication, the instructions should state specific steps to be taken and certified. If the work is to be done by professional services, either in-house or outside, the instruction should inform the custodian where the media should be delivered, and what certification paperwork is required.



Strategic Points:

The work group formulating the document retention program and implementation plan should consider automating the data-destruction process. For data, this would entail using networked technology to wipe or eradicate data once it ages. For documents, an automated destruction protocol might move documents out to an archive at a certain age, and later from archive to destruction.

 Cross Reference:

Sample destruction protocols, see 16.20, 16.21.

16.11[4] Implementation Plan Should Provide Special Procedures for Sensitive or Confidential Information.

Sensitive information often requires special destruction procedures.

Example--Sensitive or Confidential Documents:

Regulations under the Health Insurance Portability and Accountability Act ("HIPAA") require that medical care entities "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information" [45 *CFR* § 164.530(c)]. These safeguards can include shredding documents that contain covered information before discarding them [see U.S. Dep't of Health & Human Servs., Summary of the HIPAA Privacy Rule, at 14 (1003), <http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf>].

Consider:

Deletion of sensitive information stored in electronic form will not be sufficient if paper copies of the information remain. Sensitive paper documents should at least be shredded, if not criss-cross shredded and incinerated. If an organization generates paper documents that contain sensitive or confidential information, and lacks the capacity to perform this kind of destruction, it should consider contracting with a disposal firm that can take outdated documents on a monthly or bi-monthly basis and certify destruction. The organization should keep the destruction documentation for an appropriate period of time.



13 of 22 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 16 Establishing Best Practices Regarding Electronically Stored Information

III. CREATING DOCUMENT RETENTION PROGRAM

1-16 MB Practice Guide: CA E-Discovery and Evidence 16.12

AUTHOR: Diane E. Barry, Esq.

16.12 Document Retention Program Should Include Rollout Plan.

16.12[1] Proper Rollout Is Important to Success of Program. Once the document retention program has been created, it must be rolled out in a disciplined fashion. Rollout must take into account the size of the organization and the current state of the organization's legal affairs.



Warning:

If the document retention program is not properly rolled out and implemented, the organization is in some ways worse off than if it had no program at all. The existence of the program will serve as proof that the organization is aware of its duties, but the failure to implement the program will be evidence that the organization has not complied with those duties.

Consider--Removable Storage Media:

One of the most difficult media groups to inventory, categorize, and track is removable storage media--items such as floppy disks, CDs, and USB drives. They are small, are created and maintained by individual users, are maintained off the company's network, and are not within reach of automated tools for categorization and maintenance. All of these characteristics make them difficult to locate, inventory, and manage. Current employees should be held accountable to manage their own removable media. Media from exiting employees should be boxed and sent to a central authority for review, categorization, and either archiving or destruction. The most problematic items are usually unclaimed media left in uncontrolled areas (work rooms, conference rooms, guest offices, storage rooms, former employee work areas). Bringing this set of media into the program usually requires an office-by-office search and a concerted effort to review, categorize, and treat the media



Cross References:

Discussion of incremental rollout for large organization, see 16.12[2].

Discussion of effect of pending litigation on rollout, see 16.12[3].

16.12[2] Rollout in Large Organization Typically Is Done Incrementally. Many organizations choose to roll out in increments. The two most common approaches are the following:

- Rolling out by department or business unit. This approach permits the organization to find an easy place to start, and to apply lessons learned to the more difficult departments as it progresses.
- Applying the new document retention program to all new documents, and cleaning out past archives and files over time. This approach makes for a clean program going forward, and gives time to clear out problems left behind.

16.12[3] Rollout Must Not Disturb Existing Litigation Holds. Rollout of the program must take into account any litigation hold duties already in place at the organization. Ordinarily, rollout should be delayed for employees or departments involved in litigation. If the rollout must include departments with documents currently subject to litigation-preservation duties, special care and precautions should be taken to identify documents that must be preserved outside of the document retention program, and those documents should be exempt from any purging or scheduled deletion efforts until further notice from the organization's counsel.



Cross References:

Litigation holds, see *Ch. 5, Initial Procedures in E-Discovery--Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference*, 5.06, 5.07.



14 of 22 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 16 Establishing Best Practices Regarding Electronically Stored Information

III. CREATING DOCUMENT RETENTION PROGRAM

*1-16 MB Practice Guide: CA E-Discovery and Evidence 16.13***AUTHOR:** Diane E. Barry, Esq.**16.13 Document Retention Program Should Include Compliance Program.**

16.13[1] Compliance Program Helps Ensure Effectiveness of Document Retention Program. A compliance program looks both forward and backward. The forward-looking elements educate employees so that they can comply with the document retention program and be held accountable for noncompliance. The backward-looking elements measure the current compliance level, so that education and other elements of the program can be adjusted to maximize effectiveness.

Regular training also provides a basis for establishing the organization's good faith should discoverable electronic information ever be inadvertently lost or destroyed [see CCP §§ 1985.8(l)(1), 2031.060(i)(1), 2031.300(d)(1), 2031.310(j)(1), 2031.320(d)(1)].

**Cross Reference:**

Discussion of good faith application of document retention program, see 16.06[2][c].

**Strategic Point:**

A strong retention program requires maintenance and upkeep. If an organization wishes to rely upon its program for litigation defense, it should be budgeting for ongoing retention compliance and program revisions. If it does not, opposing counsel could question the depth of the organization's commitment to its stated program.

16.13[2] Compliance Program Should Include Education Component. Employee education should be given at least annually, and should be part of training for all new employees. The goal of education programs is to assist employees in bringing their own files into compliance with the retention program, and to understand what the organization is doing when files are purged, wiped or shredded. The education program also provides a basis for holding the employee responsible for failure to comply.

Record Keeping:

The organization should document training sessions and retain date-stamped copies of training materials and handouts.

Example--Employee's Failure to Comply With Document Retention Program:

The Equal Employment Opportunity Commission (EEOC) claimed that an employer was not keeping documents regarding job applicants that it was required to retain under Title VII. Part of the corporation's defense was a fairly extensive description of its document retention program. After the trial court granted the defendant summary judgment on this issue, the Seventh Circuit reversed, pointing out that there was a question of fact whether the program was adequate, because it relied upon managers who were hiring to collect the resumes and applications and turn them over to the retention program. In this case, the manager threw out the resumes of anyone he did not hire, in direct contravention of the defendant's document retention program [*EEOC v. Target Corp.* (7th Cir 2006) 460 F3d 946, 955-956] .

16.13[3] Compliance Program Should Require Custodian Certifications. Once employees have been trained, they can be held responsible for bringing their own files into compliance with the organization's requirements. At least once each year, each custodian should be required to certify in writing that he or she has reviewed the files he or she is responsible for, and that the files comply with the requirements of the document retention program. Such certifications are a reminder to employees to be familiar with the program's requirements and that the organization takes this matter seriously. The signed certifications also provide documentary evidence that the organization has taken affirmative steps to implement its program and is giving its best efforts to complying with its program in good faith.

16.13[4] Compliance Program Should Require Periodic Audits. Employee certifications and other program metrics should be checked periodically, preferably by a group outside of the organization. The audit should at least make a check on a random selection of employee certifications to verify that actual compliance matches the certification [see, e.g., *EEOC v. Target Corp.* (7th Cir 2006) 460 F3d 946, 955-956 (employees discarded documents in violation of employer's document retention program)].

The audit process provides at least two positive assurances. First, it provides a metric to measure the effectiveness of the employee education program and the process for retention and destruction. Compliant files mean that the training process is working and that employees understand their obligations and are able to fulfill them. Noncompliant files require inquiry as to how the noncompliance occurred, and remediation should be applied as needed. Second, an audit provides additional documentary support showing the organization's commitment to its program.

16.13[5] Compliance Program Should Include Periodic Review. A document retention program must be an ongoing project, because business needs and legal requirements change, data objects change, and best practices regarding eradication and destruction change. In order for the retention program to continue to meet changing business, legal, and information technology needs, it must be reviewed at least annually, and adjusted accordingly.



15 of 22 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 16 Establishing Best Practices Regarding Electronically Stored Information
IV. MAKING USE OF DOCUMENT RETENTION PROGRAM IN DISCOVERY

1-16 MB Practice Guide: CA E-Discovery and Evidence 16.14

AUTHOR: Diane E. Barry, Esq.

16.14 CHECKLIST: Making Use of Document Retention Program in Discovery.

☐ If litigation is reasonably imminent, take steps to prevent organization's routine destruction of information that may be discoverable in litigation.

Discussion:

See 16.16[1][a]

☐ If representing organization, advise it to place hold on destruction of information under document retention program.

Authority:

Zubulake v. UBS Warburg LLC (SDNY 2004) 220 FRD 212, 218

☐ If representing opposing party, inform organization's counsel in writing that discovery of electronically stored information is reasonably likely to be sought, and demand preservation.

☐ Use organization's document retention schedule in discovery.

☐ If representing opposing party:

☐ Early in litigation, demand production of organization's document retention program, including retention schedule.

Authority:

CCP § 2031.020

- ☐ Refer to organization's document retention schedule as guide in planning further discovery.

Discussion:

See 16.17[1]

- ☐ If representing organization, use document retention schedule to help identify documents that are responsive to opposing party's discovery demands.

Discussion:

See 16.16[1][b]

- ☐ Refer to organization's document retention program as appropriate in seeking or opposing request for discovery sanctions.

Discussion:

See 16.16[2], 16.17[2]



16 of 22 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 16 Establishing Best Practices Regarding Electronically Stored Information
IV. MAKING USE OF DOCUMENT RETENTION PROGRAM IN DISCOVERY

1-16 MB Practice Guide: CA E-Discovery and Evidence 16.15

AUTHOR: Diane E. Barry, Esq.

16.15 Options and Strategies.

An organization's document retention program can be useful when the organization becomes involved in litigation.

For the organization itself, the document retention schedule provides a convenient list of custodians who can be contacted to place a litigation hold on information relevant to the litigation. The schedule also serves as a starting point for locating and gathering information and documents that are responsive to discovery demands propounded by the opposing party.

Cross Reference:

Discussion of litigation hold and organization's duty to preserve relevant information, see 16.16[1][a].

Discussion of document retention schedule as starting point for response to discovery demand, see 16.16[1][b].

For an opposing party, the organization's document retention schedule--essentially a catalogue of the kinds of information generated and maintained by the organization--can be used as a resource for planning discovery.

Cross Reference:

Discussion of document retention schedule as resource for planning discovery, see 16.17[1].

For both sides, the organization's document retention program and the circumstances of its implementation may be relevant evidence in the context of a motion for sanctions, to establish whether the organization acted in good faith in preserving or destroying relevant information [see CCP §§ 1985.8(l)(1), 2031.060(i)(1), 2031.300(d)(1), 2031.310(j)(1), 2031.320(d)(1)].

Cross Reference:

Discussion of document retention program as relevant to question whether organization acted in good faith, see 16.16[2], 16.17[2].



17 of 22 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 16 Establishing Best Practices Regarding Electronically Stored Information
IV. MAKING USE OF DOCUMENT RETENTION PROGRAM IN DISCOVERY

1-16 MB Practice Guide: CA E-Discovery and Evidence 16.16

AUTHOR: Diane E. Barry, Esq.**16.16 Organization May Use Its Document Retention Program in Responding to Discovery Demand.****16.16[1] Document Retention Program Assists in Preventing Loss of Responsive Information.**

16.16[1][a] Organization Has Duty to Preserve Materials Relevant to Litigation. The destruction of relevant information after the commencement of litigation is sanctionable as a misuse of discovery [*New Albertsons, Inc. v. Superior Court* (2008) 168 CA4th 1403, 1429-1430, 86 CR3d 457, 477-478 ; see CCP § 2023.030]. Consequently, the organization has an affirmative duty to create effective measures to respond to discovery obligations and communicate those obligations to the employees who have possession of discoverable materials so they can place a litigation hold on the information and any scheduled destruction of it [*National Ass'n of Radiation Survivors v. Turnage* (ND Cal 1987) 115 FRD 543, 557-558] . Once an organization is on notice that it must act to preserve relevant materials, it must act quickly to implement a litigation hold and preserve even outdated relevant materials [see *UMG Recordings, Inc. v. Hummer Winblad Venture Partners (In re Napster, Inc. Copyright Litig.)* (ND Cal 2006) 462 F Supp2d 1060, 1070] .

**Timing:**

The duty to preserve evidence attaches arises when the party has notice that the evidence is relevant to litigation or when a party should know that the evidence may be relevant to future litigation [see *Fujitsu v. Federal Express Corp.* (2d Cir. 2001) 247 F3d 423, 436 ; *Zubulake v. UBS Warburg LLC* (SDNY 2003) 220 FRD 212, 216] . A party or anticipated party must retain all relevant documents in existence at the time the duty to preserve attaches, and any relevant documents created thereafter [see *Zubulake v. UBS Warburg LLC* (SDNY 2003) 220 FRD 212, 218] .

**Cross Reference:**

Meet and confer notices and preservation demands, 5, Initial Procedures in E-Discovery: Notice, Document Preservation, Meeting and Conferencing, and Case Management Conference, 5.09-5.21.

16.16[1][b] Document Retention Schedule Provides Starting Point for Litigation Hold or Responding to Discovery Demands. Because a document retention schedule lists all information the organization generates and gathers, where it is located, and who is in charge of deleting information, it is a very effective place to begin a litigation

hold effort or a search for information that is responsive to a discovery demand. Categories of information can be preserved, or gathered for purposes of providing discovery, by contacting the listed custodians.



Cross References:

Discussion of contents of document retention schedule, see 16.10[2]-[4].

Litigation holds, see *Ch. 5, Initial Procedures in E-Discovery: Notice, Document Preservation, Meeting and Conferring, and Case Management Conference*, 5.03-5.13.



Warning:

A failure to send a litigation hold notice to appropriate custodians, and to follow up with persons to whom the notice was sent, is sanctionable if it results in the spoliation or destruction of relevant material [see *National Ass'n of Radiation Survivors v. Turnage* (ND Cal 1987) 115 FRD 543, 557-558] .

16.16[2] Document Retention Program Provides Basis for Good Faith Defenses. If relevant electronically stored information is destroyed or otherwise lost during the period when the organization has a duty to preserve it, the organization will not be sanctioned if it can establish that the loss occurred as the result of the routine, good faith operation of an electronic information system, unless there are exceptional circumstances justifying sanctions [see *CCP §§ 1985.8(l)(1), 2031.060(i)(1), 2031.300(d)(1), 2031.310(j)(1), 2031.320(d)(1)*]. In contrast, if the information was destroyed for the purpose of keeping it out of the litigation, the destruction is sanctionable [see *United States v. Philip Morris USA, Inc.* (DDC 2004) 327 F Supp2d 21, 23-25] . Good faith compliance with an existing document retention program may help the organization establish that any destruction or loss of information occurred in the routine, good faith operation of the organization's electronic information system [see *Arthur Andersen LLP v. United States* (2005) 544 US 696, 704, 125 S Ct 2129, 161 L Ed2d 1008 (destruction of document in compliance with valid document retention policy is not wrongful under ordinary circumstances); *Martinez v. Abbott Labs.* (7th Cir 2006) 171 Fed Appx 528, 531 (destruction of document in normal course of business does not prove demonstrate bad faith)].



Cross Reference:

Discussion of seeking or opposing sanctions, see *Ch. 13, Seeking or Opposing Sanctions for Noncompliance*.



18 of 22 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 16 Establishing Best Practices Regarding Electronically Stored Information
IV. MAKING USE OF DOCUMENT RETENTION PROGRAM IN DISCOVERY

1-16 MB Practice Guide: CA E-Discovery and Evidence 16.17

AUTHOR: Diane E. Barry, Esq.

16.17 Opposing Party May Use Organization's Document Retention Program to Obtain Discovery.

16.17[1] Document Retention Schedule May Assist in Identifying Discoverable Information. Obtaining the opposing party's document retention schedule early on in litigation can be useful in planning further discovery, since the schedule will list all the information the party routinely generates and gathers [see *Ideal Aerosmith, Inc. v. Acutronic USA, Inc.* (WD Pa 2008) 2008 US Dist LEXIS 85619, at *8 ("It is commonplace in litigation to inquire of a corporate defendant the steps it took to find and produce documents relating to the litigation, as well as the corporation's electronic document storage and retrieval systems, in order to ensure that discovery was diligently completed.")]



Cross Reference:

Discussion of contents of document retention schedule, see 16.10[2]-[4].

16.17[2] Document Retention Program May Provide Basis for Inference of Bad Faith. If relevant documents are destroyed when a party had a duty to preserve them, a court considering sanctions can look to compliance with a document retention policy to assist in determining whether the destruction was done in bad faith and is therefore sanctionable [see *United States v. Philip Morris USA, Inc.* (DDC 2004) 327 F Supp2d 21, 23-25 (employees deleted e-mails in violation of court order and company document retention policy); *Broccoli v. Echostar Commc'ns Corp.* (D Md 2005) 229 FRD 506, 512 (defendant "clearly acted in bad faith in its failure to suspend its email and data destruction policy or preserve essential personnel documents in order to fulfill its duty to preserve the relevant documentation for purposes of potential litigation")].



19 of 22 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 16 Establishing Best Practices Regarding Electronically Stored Information
V. FORMS

1-16 MB Practice Guide: CA E-Discovery and Evidence 16.18

AUTHOR: Diane E. Barry, Esq.

16.18 Sample Document Retention Policy.

DOCUMENT RETENTION POLICY OF _____[*name of organization, e.g., MARY JONES ENTERPRISES, INC.*]

DOCUMENT RETENTION POLICY OF _____[*name of organization, e.g., MARY JONES ENTERPRISES, INC.*]

Effective _____[*date*]

I. Purpose

In accordance with the Sarbanes-Oxley Act, which makes it a crime to alter, cover up, falsify, or destroy any document with the intent of impeding or obstructing any official proceeding, this policy provides for the systematic review, retention, and destruction of documents received or created by this organization in connection with the transaction of its business. This policy covers all records and documents, regardless of whether they have a physical form or consist of electronically stored information.

This policy is designed to ensure compliance with federal and state laws and regulations, and to eliminate accidental or innocent destruction of records and to facilitate the organization's business by promoting operational efficiency and freeing up valuable storage space.

II. Document Retention

The organization follows the document retention procedures outlined below. If your department has categories of documents that are not listed below, please contact _____[*name*], at extension _____, so that the Retention Committee can amend this policy to address the needs of your department.

III. Corporate Records

1-16 MB Practice Guide: CA E-Discovery and Evidence 16.18

Accident Reports and Workers' Comp Records	5 years
Accounting and Corporate Tax Records	7 years
Annual Audits and Financial Statements	7 years
Articles of Incorporation	Permanent
Bank Records (statements, deposit slips, etc.)	7 years
Board Meeting and Board Committee Minutes	Permanent
Board Policies/Resolutions	Permanent
Business Expense Records	7 years
By-laws	Permanent
Construction Documents	Permanent
Contracts Files (after expiration)	7 years
Corporate Credit Card Receipts	3 years
Correspondence (general)	3 years
Depreciation Schedules	7 years
Document Retention Policy & Schedules	Permanent
Employee HR Files	3 years after termination
Employment & Termination Agreements	Permanent
Employment Applications	3 years
Environmental Studies and Work Files	Permanent
Fixed Asset Records	Permanent
Franchise Tax Board Returns and Associated Work Papers	7 years
Garnishment Records	7 years
General Ledgers	7 years
I-9 Forms	3 years after termination
Insurance Policies	Permanent
Invoices	7 years
IRS Tax Returns and Associated Work Papers	7 years
Journal Entries	7 years
Leases	6 years after expiration
Legal, Insurance, and Safety Records	Permanent
Payroll and Employment Tax Records	7 years
Petty Cash Vouchers	3 years
Real Estate Transactional Documents	Permanent
Retirement and Pension Plan Documents	Permanent
Sales Records	5 years
Stock and Bond Records	Permanent

IV. Crisis Planning

The organization's records will be stored in a safe, secure, and accessible manner. Documents and financial files that are essential to keeping the organization operating in an emergency will be duplicated or backed up at least every week and maintained off site. _____ *[If available, add reference to additional protocol that describes emergency and crisis practices, such as backup, storage, and restoration.]*

V. Compliance

A list of the organization's requirements regarding proper use, storage, and retention of corporate information are attached as Exhibit 1 _____. *[not provided with this form--exhibit must be organization-specific document]*. As noted on Exhibit 1, some of the listed requirements are to be applied across the entire organization, while others apply only to particular departments.

The organization will conduct employee training regarding the organization's requirements as stated in Exhibit 1 quarterly every year. Every employee of the organization shall be required to attend at least one training session each year.

Every employee is responsible for maintaining the corporate records in their custody and control in accordance with company policies regarding records. On _____ *[date]*, every employee shall be required to certify that the records within their custody and control conform to corporate requirements.

VI. Destruction

The organization's _____ *[title of executive]* is responsible for the ongoing process of identifying its records that have met the required retention period and overseeing their destruction.

Each of the corporate record custodians listed in the Document Retention Schedule is responsible for organizing the destruction of the records assigned to them in the schedule, as they reach the end of the retention period. The protocols for destruction of records are listed in the Document Retention Schedule that is attached to this Document Retention Policy as Exhibit 2. Once destruction has been accomplished in accordance with the Document Retention Schedule, a certification shall be provided to the _____ *[title of executive]*.

VII. Compliance

Failure on the part of employees to follow this policy can result in possible civil and criminal sanctions against the organization and its employees, and possible disciplinary action against responsible individuals. The _____ *[title of executive]* and finance committee chair will periodically review these procedures with legal counsel and/or the organization's certified public accountant to ensure that they are in compliance with new or revised regulations.

Exhibit 1: Proper Use, Storage, and Retention of Corporate Information

[Attach description of company-specific requirements]

NOTES:

Checklist:

See 16.07

Discussion:

See 16.09

Related Form for Document Retention Schedule:

See 16.19



20 of 22 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 16 Establishing Best Practices Regarding Electronically Stored Information
V. FORMS*1-16 MB Practice Guide: CA E-Discovery and Evidence 16.19***AUTHOR:** Diane E. Barry, Esq.**16.19 Sample Document Retention Schedule.**

Document Category	Retention Period	Custodian	Approved Disposal Protocol
Accident Reports & Workers Comp Records	5 years	TITLE (Include name, e-mail and phone ext of current title holder).	Paper Records: Shredding Protocol 2--for Disposal of Sensitive Records
Locations: Paper files: HR File Cabinet 2		Electronic Records: Data Wipe Protocol 2 (sensitive information).	
ESI: Peoplesoft database located on server H98493			
Accounting and Corporate Tax Records	7 years	TITLE (Include name, e-mail and phone ext of current title holder).	Paper Records: Shredding Protocol 2--for Disposal of Sensitive Records
Locations: Paper files: Accounting Department File drawers 4, 9, and 22.		Electronic Records: Data Wipe Protocol 2 (sensitive information).	
ESI: Oracle database, loc-			

1-16 MB Practice Guide: CA E-Discovery and Evidence 16.19

ated on servers A84930 and
A73625

Bank Records (statements, 7 years
deposit slips, etc.)

TITLE (Include
name, e-mail and
phone ext of current
title holder).

Paper Records:
Shredding Protocol 2--for Disposal
of Sensitive Records

Location:
Paper records only (no ESI)
Iron Mountain--see Index

Electronic Records:
Data Wipe Protocol
2 (sensitive informa-
tion).

Desert Construction Project 10 years post
5 south wall brick samples project opening

TITLE (Include
name, e-mail and
phone ext of current
title holder).

Delivery to Santos Pulverization
Co. for permanent destruction per
Construction Samples Disposal
Policy 5 (non-asbestos bricks, ce-
ment blocks).

Contracts Files (after expira- 7 years
tion)

TITLE (Include
name, e-mail and
phone ext of current
title holder).

Paper Records:
Shredding Protocol 1--for Disposal
of Ordinary Records

Electronic Records:
Data Wipe Protocol 1 (Ordinary In-
formation).

NOTES:

Checklist:

See 16.07

Discussion:

See 16.10

Related Form for Document Retention Policy:

See 16.18



21 of 22 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 16 Establishing Best Practices Regarding Electronically Stored Information
V. FORMS

1-16 MB Practice Guide: CA E-Discovery and Evidence 16.20

AUTHOR: Diane E. Barry, Esq.

16.20 Sample Protocol for Destruction of Sensitive Paper Documents.

Checklist for Records Disposal
Sensitive Paper Documents

- ☐ The records are eligible for destruction according to the _____ [name of organization] Document Retention Policy.
- ☐ The records are not needed to support current or imminent litigation actions, government investigations, audits, or public disclosure requests. (If in doubt, please contact the office of the _____ [name of organization] General Counsel before destruction.)
- ☐ The records are **not** designated as "Archival" or "Potentially Archival" on the document retention schedule.
- ☐ Documentation of the disposal will be created, filed, and retained in the appropriate file and includes the date the records were disposed of, and a description of the records (including their dates, official titles, and retention periods).
- ☐ Files were delivered with a properly filled-out Records Destruction Form describing the records and their age.
- ☐ The documents are from a category listed on the Document Retention Schedule as requiring special handling for sensitive information.

☐ Cross-shred the documents using the criss-cross shredder designated for this purpose in the archive department.

☐ Gather cross-shredded document shreds and dispose of shreds in the red, locked "INCINERATE" hamper located in the archive department.

☐ Fill out destruct method and date certification spaces at the bottom of the Records Destruction Form, and sign the certification line.

☐ Retain a copy of the form, and send the original to _____ [*title of executive in charge of retention and destruction*] through the interoffice mail.

NOTES:

Checklist:

See 16.07

Discussion:

See 16.11[4]

Related Form for Document Retention Policy:

See 16.18

Related Form for Document Retention Schedule:

See 16.19

Related Form for Data-Wipe Protocol for Hard Drives:

See 16.21



22 of 22 DOCUMENTS

Matthew Bender Practice Guide: California E-Discovery and Evidence

Copyright 2010, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Chapter 16 Establishing Best Practices Regarding Electronically Stored Information
V. FORMS*1-16 MB Practice Guide: CA E-Discovery and Evidence 16.21***AUTHOR:** Diane E. Barry, Esq.**16.21 Sample Data-Wipe Protocol for Hard Drives.**Computer Serial Num-
ber:Hard Drive Serial Num-
ber:

Date Received:

Received From:

Received By:

Secure Storage
Location:

Purpose:

Complete wipe of hard
drive in preparation for
recycling or disposal, as
prescribed by corporate
document retention
policy.***Document Retention Compliance******A. Computer Verification***

Verify that Computer serial number matches serial number on form above.

Serial number matches:

Yes

No

If the serial number does not match, return the computer to the person who delivered it and sign below:

Computer serial number does not match documentation provided.
Technician Signature:

Delivered By:	Delivered To:	Date Delivered:
Name:	Name:	
Employee ID:	Employee ID:	

B. Document Retention Approval Verification

Was the hard drive delivered by the custodian designated in the corporate document retention policy? Current policy revision date: 08/31/09 _____.

Yes	_____	No	_____
	_____		_____

If the hard drive was not delivered by the appropriate custodian please contact _____ and hold the hard drive in secure storage pending approval for wipe.

If the drive is not approved for wipe, it should be returned to the person who delivered it.

If it is approved for wipe, the appropriate custodian must sign below before you can proceed:

The above computer is approved for data wipe in preparation for recycling or disposal, as prescribed by corporate document retention policy:

Date: _____

Custodian name: _____

Employee ID: _____

C. Computer Wipe Procedure

This protocol requires use of the following items:

1. EnCase(R) software kit (stand alone or enterprise version).
2. Tool kit for disassembly of computer casing.

Instructions

1-16 MB Practice Guide: CA E-Discovery and Evidence 16.21

1. Disassemble exterior of computer to gain access to target hard drive.
2. Verify that hard drive serial number matches paperwork at the top of this form.

Serial number matches:

Yes _____ No _____

If serial number does not match, reassemble the computer and place in secure storage. Contact _____ and inform of problem. Await delivery of proper paperwork before proceeding.

If serial number does match, proceed to step 3.

3. Remove hard drive.
4. Attach target hard drive directly to technician computer with EnCase tool.
5. From EnCase, select the Wipe Drive option from the "Tools" pull-down menu.
6. Conduct a forensic wipe from bit zero to bit end.
7. Repeat steps 5 and 6.
8. Use EnCase in preview mode to preview the drive and ensure that all data has been wiped.
9. Reassemble computer.
10. Fill out paperwork below, and forward computer to _____ in records retention for further action.

Instructions to Technician:

Date Data Wipe Was Performed: Signature of Technician:

 Name:

Employee ID:

Delivered To:

Delivery Date:

Computer is intended for:

Disposal: _____

Recycling: _____

Disposal:

Delivered To:

Date:

Recycling:

Delivered To:

Date:

- Retain one final copy of this form for your annual records file.
- Send one final copy of this form to: _____ in records retention.

NOTES:

Checklist:

See 16.07

Discussion:

See 16.11[3]

Related Form for Document Retention Policy:

See 16.18

Related Form for Document Retention Schedule:

See 16.19

Related Form for Protocol for Destruction of Sensitive Paper Documents:

See 16.20

Source of Form:

Diane E. Barry, Esq., Director--Discovery Strategy and Management, International Litigation Services,
and Gene R. Cioni, Chief Data Investigator, International Litigation Services